

Windows IT Pro

JUNE 2011 | WINDOWSITPRO.COM | WE'RE IN IT WITH YOU

Exchange Server Deployment

Choose Your Option p. 23



Microsoft's Rajesh Jha

Talks About the Future of Exchange p. 29

Configure Virtual Disk Options:

Hyper-V p. 41

VMware ESX p. 43

**Manage Network Drives
with WSH Scripts** p. 34

**Integrate Mobile Platforms
with Exchange 2010** p. 45

**DirectAccess Improvements
in Forefront UAG SP1** p. 37

SharePoint 2010 Goes Social:
The User Profile Service p. 49

Digital Edition Copyright Notice

The content contained in this digital edition ("Digital Material"), as well as its selection and arrangement, is owned by Penton Media, Inc. and its affiliated companies, licensors, and suppliers, and is protected by their respective copyright, trademark and other proprietary rights.

Upon payment of the subscription price, if applicable, you are hereby authorized to view, download, copy, and print Digital Material solely for your own personal, non-commercial use, provided that by doing any of the foregoing, you acknowledge that (i) you do not and will not acquire any ownership rights of any kind in the Digital Material or any portion thereof, (ii) you must preserve all copyright and other proprietary notices included in any downloaded Digital Material, and (iii) you must comply in all respects with the use restrictions set forth below and in the Penton Privacy Policy and the Penton Terms of Use (the "Use Restrictions"), each of which is hereby incorporated by reference. Any use not in accordance with, and any failure to comply fully with, the Use Restrictions is expressly prohibited by law, and may result in severe civil and criminal penalties. Violators will be prosecuted to the maximum possible extent.

You may not modify, publish, license, transmit (including by way of email, facsimile or other electronic means), transfer, sell, reproduce (including by copying or posting on any network computer), create derivative works from, display, store, or in any way exploit, broadcast, disseminate or distribute, in any format or media of any kind, any of the Digital Material, in whole or in part, without the express prior written consent of Penton Media, Inc. To request content for commercial use or Penton's approval of any other restricted activity described above, please contact the Reprints Department at (888) 858-8851. Without in any way limiting the foregoing, you may not use spiders, robots, data mining techniques or other automated techniques to catalog, download or otherwise reproduce, store or distribute any Digital Material.

NEITHER PENTON NOR ANY THIRD PARTY CONTENT PROVIDER OR THEIR AGENTS SHALL BE LIABLE FOR ANY ACT, DIRECT OR INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF OR ACCESS TO ANY DIGITAL MATERIAL, AND/OR ANY INFORMATION CONTAINED THEREIN.

Microsoft

Let's talk optimizing applications, not just servers.

Windows Server is changing the conversation.

Windows Server Hyper-V and System Center let you manage your infrastructure as a pool of computing resources: a private cloud. This gives you control beyond virtualization, letting you monitor application performance and allocate computing power as needed, so applications run at their maximum efficiency. The power to control your resources, rather than being controlled by them. **That's Cloud Power.**

Find out more about our private cloud solutions.
Microsoft.com/cloud/privatecloud

Scan our tag
or text ITPRO1
to 70700*.

Get the free
mobile app from
<http://gettag.mobi>



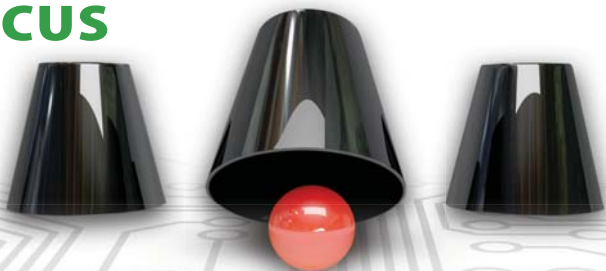
*Standard messaging and data rates apply.



Cloud Power

 Windows Server
Hyper-V

FOCUS



23 Exchange Server Deployment Options

Many alternatives are available for implementing Exchange in your environment, including traditional deployment, virtualization, cloud-based solutions, and a combination of these approaches. To find the best solution for your organization, you need to consider the benefits and caveats of each option.

BY MICHAEL B. SMITH

29 Microsoft's Rajesh Jha Talks About the Future of Exchange

Microsoft's Rajesh Jha discusses the growing role of the cloud in the future development of Exchange Server, but he also stresses the importance of listening to customer's requirements and embracing change.

BY B.K. WINSTEAD

COLUMNS

OTEY | IT PRO PERSPECTIVES



4 Is the Cloud Really Just the Return of Mainframe Computing?

Cloud services offer a host of advantages for businesses, but organizations have been slow to jump on the bandwagon. Learn why many companies have a "been there, done that" attitude toward the cloud.

JAMES | BUSINESS TECHNOLOGY PERSPECTIVES



5 Why the Cloud is Here to Stay

Despite very strong opinions on both sides, cloud computing shouldn't be an all or nothing proposition.

THURROTT | NEED TO KNOW



7 Office 365 for Small Business and Celebrating SharePoint's Tenth

Learn why Office 365 is a no-brainer for small business—and maybe for the enterprise as well—plus, what has Microsoft really created with SharePoint?

MINASI | WINDOWS POWER TOOLS



11 Fix Unbootable Systems with Bootsect

If you have a non-booting system, sometimes it's best to get back to basics. Here's how to use Bootsect to investigate the MBR and the so-called "Windows Boot Record" for anomalies.

OTEY | TOP 10



13 Cluster Shared Volume FAQs

Cluster Shared Volumes (CSVs), introduced with Windows Server 2008 R2,

let multiple cluster nodes concurrently access shared storage. Find out answers to common questions such as what limitations they have and what network requirements they impose.

DEUBY | ENTERPRISE IDENTITY



14 First Steps in Federation

Want to get some hands-on experience with federation? Try spending some time

with the *AD FS 2.0 Step-by-Step and How To Guides*.

NAIR | WHAT WOULD MICROSOFT SUPPORT DO?



16 Tips for Troubleshooting Remote Desktop Connection Problems

There are many reasons why you might be having trouble while attempting to connect to a remote computer. In this checklist, you'll find the most common problems that the Microsoft support team sees.

Windows IT Pro

A PENTON PUBLICATION

JUNE 2011
VOLUME 17 NO 6

FEATURES

34 Manage Network Drives with WSH Scripts

The WshNetwork and FileSystemObject objects are a dynamic duo when you need to work with mapped drives in Windows Script Host (WSH) scripts.

BY ROB GRAVELLE

37 DirectAccess Improvements in Forefront Unified Access Gateway SP1

Forefront UAG SP1 incorporates several improvements in DirectAccess support, including "always managed" functionality, native support for Force Tunneling, one-time password (OTP) authentication, enhanced monitoring and logging capabilities, and easier deployment.

BY FERNANDO CIMA

41 Hyper-V Disk Configuration Options

Hyper-V offers a wide range of options for configuring VM disks: IDE or SCSI, fixed or dynamic, VHD or pass-through. Although there's no strictly correct combination of options, you should plan your configuration carefully to avoid potential problems.

BY GREG SHIELDS

43 VMware ESX Disk Configuration Options

Options to consider in VMware virtual machine (VM) disk configuration include raw device mapping, thin versus thick provisioning, IDE versus SCSI, DAS versus SAN storage, persistent versus nonpersistent independent disks, and storage group block size.

BY ALAN SUGANO

45 Integrating Mobile Platforms with Exchange Server 2010

Determining which mobile platform best integrates with Exchange 2010 can be difficult, especially because the current solutions all have limitations. The author compares Windows Mobile 6.5, Windows Phone 7, iOS 4.3, and Android 2.2 to help you make the best decision for your environment.

BY DAMIR DIZDAREVIC

49 SharePoint 2010 Goes Social, Part 1

Why you should use SharePoint's User Profile Service in social networking

BY KEVIN LAHNS

INTERACT

18 Reader to Reader

Just like deploying multiple PCs, deploying multiple iPhones, iPods, or iPads requires some additional planning and steps. Here's what you need to do.

20 Ask the Experts

Learn to configure SQL Server 2008's memory usage, add SP1 to your Windows 7 images, run Internet Explorer instances that don't share logons, and customize the Outlook 2010 status bar.

PRODUCTS

52 New & Improved

Check out the latest products to hit the marketplace.

PRODUCT SPOTLIGHT: Centrifry Suite 2011

REVIEW

53 Paul's Picks

See why Windows Phone 7 is languishing in spite of its innovative nature; and whether you should buy the thinnest, most elegant 13-inch laptop known to man.

BY PAUL THURROTT

REVIEW

54 System Mechanic Business 10

The author tested this repair tool to see if it lives up to the company's claims to automatically fix and speed up PCs.

BY MICHAEL DRAGONE

COMPARATIVE REVIEW

56 Mac-to-AD Integration

Solutions

If you want to manage your Apple Macintosh clients like you manage your Windows clients, check out these software solutions.

BY ERIC B. RUX

BUYER'S GUIDE

61 SharePoint Migration

Looking for a migration solution? Compare SharePoint migration product features in this guide.

BY CAROLINE VON DER MARWITZ

65 Industry Bytes

Updates on Exchange 2010, Lync, and more from Exchange Connections; take a tour of HP's new sustainable energy data center; and see what Windows 8 security features have bubbled up in the news.

IN EVERY ISSUE

71 Directory of Services

71 Advertising Index

71 Vendor Directory

72 Ctrl+Alt+Del



Windows IT Pro

EDITORIAL

Editorial and Custom Strategy Director

Michele Crockett mrockett@windowsitpro.com

Editor in Chief

Amy Eisenberg amy@windowsitpro.com

Senior Technical Director

Michael Otey motey@windowsitpro.com

Technical Director

Sean Deuby sdeuby@windowsitpro.com

Senior Technical Analyst

Paul Thurrott news@windowsitpro.com

Industry News Analyst

Jeff James jjames@windowsitpro.com

Custom Group Editorial Director

Dave Bernard dbernard@windowsitpro.com

Developer Content

Anne Grubb agrubb@windowsitpro.com

Exchange & Outlook

Brian Winstead bwinstead@windowsitpro.com

Networking, Storage, Hardware

Jason Bovberg jbovberg@windowsitpro.com

SharePoint

Caroline cmarwitz@windowsitpro.com

von der Marwitz

SQL Server

Megan Keller mkeller@windowsitpro.com

Systems Management, Virtualization, Windows OS

Zac Wiggy zwiggy@windowsitpro.com

Editorial Web Architect

Brian Reinholz breinholz@windowsitpro.com

CONTRIBUTORS

SharePoint and Office Community Editor

Dan Holme danh@intelliem.com

Senior Contributing Editors

David Chernicoff david@windowsitpro.com

Mark Joseph Edwards mje@windowsitpro.com

Kathy Ivens kiveness@windowsitpro.com

Mark Minasi mark@minasi.com

Paul Robichaux paul@robichaux.net

Mark Russinovich mark@sysinternals.com

Contributing Editors

Alex K. Angelopoulos aka@mvps.org

Sean Deuby sdeuby@windowsitpro.com

Michael Dragone mike@mikerochip.com

Jeff Felling jeff@blackstatic.com

Brett Hill brett@iisanswers.com

Darren Mar-Elia dmarelia@windowsitpro.com

Tony Redmond 12knocksinna@gmail.com

Ed Roth eroth@windowsitpro.com

Eric B. Rux ericbux@whshelp.com

John Savill john@savilltech.com

William Sheldon bsheldon@interknowlogy.com

Randy Franklin Smith rsmith@montereytechgroup.com

Curt Spanburgh cspanburgh@scg.net

Orin Thomas orin@windowsitpro.com

Douglas Toombs help@toombs.us

Ethan Wilansky ewilansky@windowsitpro.com

ART & PRODUCTION

Production Director

Linda Kirchesler linda@windowsitpro.com

Senior Graphic Designer

Matt Wiebe matt.wiebe@penton.com

ADVERTISING SALES

Publisher

Peg Miller pmiller@windowsitpro.com

Business Development Director

Kerry Gates kerry.gates@penton.com

EMEA Managing Director

Irene Clapham irene.clapham@penton.com

Director of IT Strategy and Partner Alliances

Birdie J. Ghiglione birdie.ghiglione@penton.com
619-442-4064

Online Sales and Marketing Manager

Dina Baird dina.baird@penton.com

Key Account Director

Chrissy Ferraro christina.ferraro@penton.com
970-203-2883

Account Executives

Barbara Ritter barbara.ritter@penton.com
858-367-8058

Cass Schulz cassandra.schulz@penton.com
858-357-7649

Client Project Managers

Michelle Andrews 970-613-4964
Kim Eck 970-203-2953

Ad Production Supervisor

Glenda Vaught glenda.vaught@penton.com

MARKETING & CIRCULATION

Customer Service service@windowsitpro.com

IT Group Audience Development Director

Marie Evans marie.evans@penton.com

Marketing Director

Sandy Lang sandy.lang@penton.com

CORPORATE



Chief Executive Officer

Sharon Rowlands sharon.rowlands@penton.com

Chief Financial Officer/Executive Vice President

Nicola Allais nicola.allais@penton.com

TECHNOLOGY GROUP

Senior Vice President, Technology Media Group

Kim Paulsen kpaulsen@windowsitpro.com

Windows®, Windows Vista®, and Windows Server® are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries and are used by Penton Media under license from owner. *Windows IT Pro* is an independent publication not affiliated with Microsoft Corporation.

WRITING FOR WINDOWS IT PRO

Submit queries about topics of importance to Windows managers and systems administrators to articles@windowsitpro.com.

PROGRAM CODE

Unless otherwise noted, all programming code in this issue is © 2009, Penton Media, Inc., all rights reserved. These programs may not be reproduced or distributed in any form without permission in writing from the publisher. It is the reader's responsibility to ensure procedures and techniques used from this publication are accurate and appropriate for the user's installation. No warranty is implied or expressed.

LIST RENTALS

Contact MeritDirect, 333 Westchester Avenue, White Plains, NY or www.meritdirect.com/penton.

REPRINTS

Diane Madzelonka, Diane.madzelonka@penton.com,
216-931-9268, 888-858-8851

VENDORS: ADD A REVENUE STREAM BY OFFERING ESCROW TO YOUR CUSTOMERS!



CAN YOU TAKE THE RISK



Affordable High-Tech Digital Escrow

Tower 48 is the most advanced and affordable digital escrow solution available. Designed and built specifically for software and other digital assets, Tower 48 makes escrow inexpensive and hassle free. Better yet, as a vendor, you can turn escrow into a service you offer to your customers and create a new revenue stream for yourself.

Regardless of whether you are a vendor who wants to offer this service to their customers, or whether you are a customer looking for extra protection, visit our web site to start a free and hassle-free trial account or to learn more about our services and digital escrow in general!

Readers of Windows IT Pro are eligible for a \$50 credit!
Redeem at this URL: www.Tower48.com/credit/WITP2011





Otey

IT PRO PERSPECTIVES

"Despite all the hype around the cloud, IT just isn't buying it—at least not yet."

Is the Cloud Really Just the Return of Mainframe Computing?

Back to the future: What's old is new again

These days it seems like just about every vendor is pushing its numerous and varied cloud offerings. It also seems like businesses are holding off on moving to cloud computing with just as much vigor. Everyone has heard all the different cloud sales pitches: Cloud services offer unlimited scalability, they provide global access to computing services, they eliminate the need to buy private infrastructure, they transform IT costs from CapEx to OpEx, they reduce management, they allow IT to be greener, and the list goes on.

The funny thing is that despite all the hype around the cloud, IT just isn't buying it—at least not yet. And this reluctance to jump headfirst into the cloud is reflected by many of the cloud sales specials that you see popping up. Many vendors, such as Amazon, are offering free low-level services to try to get you started with their offerings. Other vendors, such as Microsoft, are offering free trial periods to entice you to try their services.

One of the reasons businesses aren't all gaga about cloud services is that these services harken back to an era of computing that fell out of favor a decade or two ago—the era of the mainframe. If you think about it, cloud computing is a lot like the old centralized IT processing model of the past embodied by the mainframe. Computing power is moved away from the end users and into a centralized entity that's managed by someone else.

To be fair, the cloud isn't really centralized the way mainframes of the past were (and are). However, the cloud and mainframes are alike in that they both move the computing power and infrastructure governance farther from the users of those platforms.

Given the nature of cloud computing, the mainframe appears to be something like the ultimate cloud platform. Extreme scalability, availability, virtualization, and usage-based metering have been part of the mainframe for decades. And this mainframe mentality is part of the problem many organizations have with the cloud.

Businesses moved away from that model of centralized computing on purpose. Businesses, and perhaps more specifically their departments and end users, wanted more control of

their computing resources. They didn't want to share them with other business units—let alone other businesses. This is exactly what the cloud requires that you do. These factors led to the rise of distributed PC computing, client/server computing, and the web that we use today. Somewhat ironically, Microsoft was one of the leading vendors driving the push behind the distributed PC computing model and away from the centralized computing model, but today Microsoft is one of the leaders in the push to the cloud.

I know that cloud vendors would adamantly disagree with this assessment, but in some ways moving to the cloud is a bit like a step back in time. Cloud computing definitely moves much of the control of the computing resources away from the end users they service. The cloud also moves control of those resources out of the hands of IT.

This isn't the first time an attempt has been made to resurrect this centralized computing model. About a decade ago, vendors tried to sell IT on the then-hot trend of thin-client computing. IT didn't buy into that one, either—although perhaps in the long run it did herald the transition away from desktop applications to browser-based applications.

Perhaps computing trends are just like fashion, and just like those old bell bottoms from the 1960s have come back, so will the centralized computing model—as the cloud but with a modern twist. Certainly the landscape today is vastly different than it was in the era of the mainframe, or even a decade ago when thin-client computing was the media darling. Network connections are better today and the Internet, though far from perfect, is more reliable.

But the \$64,000 question around the future of cloud computing is, What do businesses really want? Do they really want to move back to a more centralized computing model in which the processing power and the control of IT resources lie outside the walls of the business, or do they prefer the more distributed, albeit more complex, model of distributed computing that we have today?



InstantDoc ID 129854

MICHAEL OTEY (motey@windowsitpro.com) is senior technical director for *Windows IT Pro* and *SQL Server Magazine* and author of *Microsoft SQL Server 2008 New Features* (Osborne/McGraw-Hill).



"Two of the most powerful aspects of the public cloud—the ability to pay only for the computing resources you use and the agility to quickly spool up additional IT resources as needed—make a powerful cost and operational argument for the cloud."

Why the Cloud Is Here to Stay

Efficient resource allocation makes a strong case for the cloud

When it comes to hype and buzzwords, nothing in the IT world has garnered as much attention as cloud computing. On one side, vendors and analysts are making breathless predictions about how the cloud will revolutionize IT, save the environment, save your company money, and put a smile on everyone's face. On the other side are nervous IT pros and server administrators who have legitimate concerns about security and identity in the cloud and who fear that the word cloud is CIO-speak for outsourcing. The reality is somewhere in the middle, and cloud computing shouldn't be an all-or-nothing proposition.

Cloud computing is a transformational technology and is increasingly being used by consumers and businesses. This isn't vendor babble or PR fluff: IBM recently reported that it expects its cloud computing sales to double in 2011 and to grow into a \$7 billion business by 2015. In December 2010, federal government CIO Vivek Kundra announced a cloud-first initiative that requires government agencies to identify three "must move" services and migrate one to the cloud by early 2012. Streaming movie behemoth Netflix runs entirely on Amazon Web Services (AWS), millions of individuals are using cloud-based Google email and Google Docs, and cloud-based CRM provider Salesforce.com has become a staple of sales departments everywhere.

That doesn't mean the public cloud is perfect for all IT applications, because there could be a host of reasons why a private cloud or more traditional IT solution might be a better option for your own organization. Legitimate issues remain regarding how the cloud can handle sensitive data, such as financial records, medical records, and other information subject to compliance and auditing regulations. That said, organizations such as the Cloud Security Alliance (www.cloudsecurityalliance.org) are working with cloud computing vendors to make steady progress on those fronts.

Cloud computing critics will point out the well-publicized failings of the cloud, from Amazon's multi-day service problems in April 2011 to the occasional Gmail outage. It's important to remember that cloud computing is a technology in its infancy, and it will have expected growing pains and issues. Likewise, internal IT departments don't always have spotless 100-percent uptime records either—IT departments across the globe are continually dealing with software incompatibilities, hardware failures, and millions of other IT gremlins.

IT professionals are wise to take my colleague Michael Otey's advice and evaluate vendor cloud computing claims with a wary, cynical eye. (See "Is the Cloud Really Just the Return of Mainframe Computing?" on page 4.) That said, I respectfully disagree with Michael on this point: Dismissing cloud computing as a fad or as a gussied up return to an earlier era of computing ignores the very real (and quantifiable) benefits that cloud computing can provide an organization that deploys it wisely. IT pros would be better served by proactively embracing cloud computing where appropriate and vigorously defending the use of internal IT resources when doing so is a better strategy. The cloud is empowering users, not driving them away from computing resources: Let's not forget how intimately connected the cloud is to mobile devices, a union that enables services and capabilities that were unthinkable even a few years ago.

Two of the most powerful aspects of the public cloud—the ability to pay only for the computing resources you use and the agility to quickly spool up additional IT resources as needed—make a powerful cost and operational argument for the cloud. If you're a web-based e-commerce business, building out the expensive internal infrastructure to handle the spike of web traffic around busy shopping seasons is a waste, because all that expensive internal IT hardware will consume power and human capital while it sits idle 360 out of 365 days of the year.

So what's an IT pro or IT leader to do about cloud computing? I'd suggest you adopt a healthy amount of my colleague's cloud computing cynicism, but simultaneously see what internal IT resources in your own organization could be good candidates for the cloud. An IT pro who fully understands the strengths (and weaknesses) of cloud computing can make the best decisions for the organization, become a broker and manager for evaluating cloud resources, and further the IT pro's career in the process.

Do you have a cloud computing success (or horror) story of your own to tell? Send your advice and suggestions to me via email at jeff.james@penton.com, and/or follow me on Twitter @jeffjames3.



InstantDoc ID 135995

JEFF JAMES (jeff.james@penton.com) is industry news analyst for *Windows IT Pro*. He was previously editor in chief of Microsoft *TechNet* magazine, was an editorial director at the LEGO Company, and has more than 15 years of experience as a technology writer and journalist.

How does eliminating the costs of 3rd party solutions sound?

Exchange Experts Tony Redmond & Paul Robichaux can help.

Join Tony and Paul at a 3-day Essentials workshop and take a practical approach to mastering Exchange 2010 - one that is immediately useful, easy to learn, and enables smooth and graceful deployments of Exchange.

Become an Exchange 2010 Maestro

May 3-5, 2011 – San Diego CA

June 13-15, 2011 – London UK

Oct 26-28, 2011 – Greenwich CT

Learn more and register at windowsitpro.com/go/exchange

WindowsITPro

"Office 365 Small Business makes Google's offering look unsophisticated and cobbled together by comparison."



Office 365 for Small Business and Celebrating SharePoint's Tenth

While the world is still struggling to crawl out from under the financial disaster of the past few years, in the tech industry at least, things are finally getting better. I see this most clearly in the resurgence in live events, where businesses are once again paying to send employees around the country or the world for IT training purposes. I attended two tech conferences in April, and May brings Microsoft's mammoth TechEd conference, being held a bit early this year in Atlanta. (I'm guessing the high heat and humidity of last year's show, in equally balmy New Orleans, had something to do with the scheduling.) Not coincidentally, as summer arrives, things are heating up on the Microsoft productivity front as well.

Office 365 for Small Business

Back in the January issue, I wrote about Microsoft Office 365 ("What You Need to Know About Microsoft Lync 2010, Office 365, IE9, and Windows Phone Carriers," InstantDoc ID 129032), which will replace Business Productivity Online Suite (BPOS) when it's released in final form later this year. At the time, Office 365 was available only in a limited, private beta. But now it's in public beta, so anyone can get in. I strongly recommend checking it out: This solution will appeal to individuals and small businesses in addition to the medium-sized businesses and enterprises that might seem more likely targets for this service.

As a quick refresher, Office 365 provides (Microsoft) hosted versions of Exchange, SharePoint, and Lync. Unlike BPOS, these are the latest, 2010-era versions of the products, with all the functional advantages the on-premises versions of the servers include.

But Office 365 has other advantages over BPOS as well: For one, it's cheaper and can be licensed for individual use, whereas BPOS required five or more client licenses per account. And Microsoft will offer Office 365 in numerous plans, with an escalating series of capabilities and monthly per-user costs, providing customers with more choice.

It's these two benefits that make Office 365 so interesting, in my opinion. Now, individuals and small businesses have access to the same Exchange, SharePoint, and Lync 2010 capabilities that were previously available only to larger and more sophisticated (and deep-pocketed) corporations.

So what's the experience like? You can find out now: The Office 365 public beta includes access to the Small Business version of the service. I've been using Office 365 since last fall, and I'm leaning toward using it going forward, both as an individual and as a

(very) small business of sorts (OK, as the writing team of me and my co-author working on our next book). And I suspect that the same things that excite me about Office 365 will drive individuals and small businesses to the product as well.

First, let's talk price: Office 365 Small Business costs \$6 per user per month. That works out to \$72 per year, or \$12 more per user per year than Google Apps for Business. Google does offer a free version of Google Apps as well, so there's an argument to be made that the smallest of businesses—and individuals, too—will simply go that route because free always trumps paid. But that's a bit simplistic, because it takes only a small amount of research to realize that Microsoft's offering is far more compelling and complete. Google's free service is also lacking some critical pieces, including uptime guarantees (if the service goes down, too bad), BlackBerry and Microsoft Outlook compatibility, and some security features.

So the real comparison comes down to whether Office 365 is worth an additional \$12 per year over Google Apps. That's a no brainer: We're talking real Exchange 2010 email, calendar, and contacts, along with full Exchange ActiveSync (EAS) policy support (see Figure 1) so you can ensure that your employees' mobile devices won't leak sensitive data if they're lost or stolen. It also includes real SharePoint 2010 collaboration and a privately-hosted version of Office Web Apps, with web-based versions of Microsoft Word, Excel, PowerPoint, and OneNote. And while this is a bit of a wild card for many new customers, in the sense that it's likely just something they're not familiar with, Office 365 also includes a hosted version of Lync, which provides nice presence and online communications capabilities that tie neatly into the other service, and, if you've got it on the desktop, the Office 2010 apps as well.

And you're going to want Office on the desktop, of course. Where higher-end, enterprise-oriented versions of Office 365

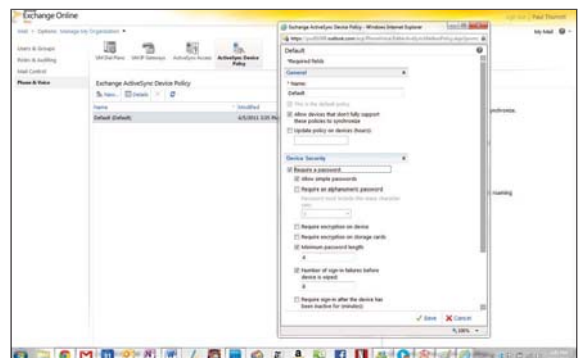


Figure 1: Configuring ExchangeActive Sync with Office 365

offer plans with subscription-based access to the full Office 2010 Professional Plus suite, with the Small Business version of Office 365, small businesses and individuals are on their own. They can use Office Web Apps, but if they have Office 2010 (or, with slightly less functionality, Office 2007) already, they can use that instead. And there's even a nice download that will auto-configure the end-user apps to work with your new online service. I was able to connect my own copies of Outlook, SharePoint Workspace, and the various productivity apps (Word, Excel, PowerPoint) to my Office 365-hosted services very easily, and setting up OneNote to sync notes to SharePoint Online was likewise a quick and simple process.

And that's another reason why this service is so exciting: For individuals and small businesses, these capabilities were so far beyond reach before that they might as well have not existed. But once you tie Office to the hosted services in Office 365, these apps come to life in ways that are both exciting and empowering to users.

The phone is a similar story. Thanks to the ubiquitous nature of EAS, connecting to your Exchange Online-based contacts, email, and calendar from any leading smart phone—iPhone, Android, Windows Phone, whatever—is straightforward. But on Windows Phone, it's even better because you can quickly link up with SharePoint Online via that device's SharePoint Workspace Mobile, part of the Office hub, and access (and edit) your documents, spreadsheets, and presentations on the go. It's the full meal deal.

What this amounts to is very powerful and professional tools at reasonable prices and a service that can make any business, no matter how small, not just look like but operate like a high-quality operation. This isn't form over function—it's the best possible function at the right price.

I do believe there's room for an even lower-end SMB version of Office 365—something that could compete with free and perhaps resemble the \$2 per user per month “kiosk” offering that Microsoft offers to Office 365 Enterprise users. But even in its current state, the Small Business version of Office 365 has quickly reestablished Microsoft's dominance in this crucial market.

Google should get some credit for getting to this market more quickly. Its

product has been hailed as being particularly well suited for small businesses that don't have the same security, integration, or cost concerns as enterprises. But Office 365 Small Business makes Google's offering look unsophisticated and cobbled together by comparison.

A Decade of SharePoint

Speaking of Office 365, one of the many things I've really enjoyed about using this product is getting to know SharePoint 2010 a bit better. SharePoint is at an interesting place this year. Microsoft says the product is officially ten years old, but its lineage is complex, and pieces of the SharePoint puzzle surely date back further than that.

SharePoint is also often credited with being Microsoft's fastest growing server product ever, and the company today claims over 100 million users, over \$1.3 billion in annual revenues, and exposure in 78 percent of the Fortune 500. So SharePoint is really a phenomenon—a platform and an ecosystem that's extremely successful and yet curiously stealthy as well: Most individuals could easily identify high-profile Microsoft products like Windows, Office, or Xbox, but to many, SharePoint is an enigma.

This is true for many people who have heard of SharePoint, too. And I think I know why: SharePoint is an amazingly versatile product, and like many similar Microsoft products—Windows, of course, but also ubiquitous applications like Outlook—it's this versatility that makes it both indispensable and hard to describe.

SharePoint's origins point to its central purpose as a document management (repository and sharing) solution, but what first caught my attention years ago was that it enabled information workers to set up their own internal collaboration sites, without requiring administrator intervention. This is such a freeing capability for users, but it also had the side effect of making SharePoint very popular with those who have access to it.

This is a trend that continues to this day: Of the users with access to SharePoint at work, over 62 percent of them actually use it. I suspect that those who use it once are quickly hooked.

According to Microsoft, the versatility of SharePoint has had some interesting

effects on the product and its users, the latter of which are now using it in ways that the product's inventors never originally envisioned. And even in my own limited experience, I've seen how the product's malleability can lead to interesting scenarios. There are traditional SharePoint sites, of course, with document libraries, lists, discussions, calendars and more. There are hosted versions of the Office Web Apps. And there are public (port 80), traditional websites. Each of these things can be interrelated, but each is also its own environment, too, and can be accessed and logically considered as separate entities.

Too, you can access SharePoint resources in such a wide variety of ways. Microsoft's free SharePoint Designer tool works just fine with SharePoint sites and websites, and if you have Office 2010 SharePoint Workspace, you can both access and sync SharePoint content to your PC, allowing offline access. Traditional Office applications—Word, Excel, PowerPoint—can easily be configured to work with SharePoint document libraries instead of the local PC, of course, and if you're lucky enough to have a Windows Phone, you get a full-featured SharePoint Workspace Mobile experience too.

I did ask Microsoft if it had any plans to extend a native SharePoint experience to other mobile platforms—and when you consider the work that Microsoft is doing on Apple's iOS platform, with apps like Bing, OneNote, and PhotoSynth, among others, it's not hard to imagine a SharePoint Workspace app on iPhones and iPads.

For now, the company says that users of non-Windows Phone 7-based mobile devices will need to access SharePoint via a mobile web browser—your mileage may vary—but that it will have more to say on this topic in the future. That's fine with me: SharePoint is so rich and versatile, I'll have a lot more to say about this product in the weeks and months ahead. I suspect this is a topic I'll be returning to again and again.



InstantDoc ID 135790

PAUL THURROTT (thurrott@windowsitpro.com) is the senior technical analyst for *Windows IT Pro*. He writes a weekly editorial for *Windows IT Pro UPDATE* (www.windowsitpro.com/email) and a daily Windows news and information newsletter called *WinInfo Daily UPDATE* (www.wininformant.com).

1,000 Oracle/Sun clients recently upgraded. To IBM Power Systems.

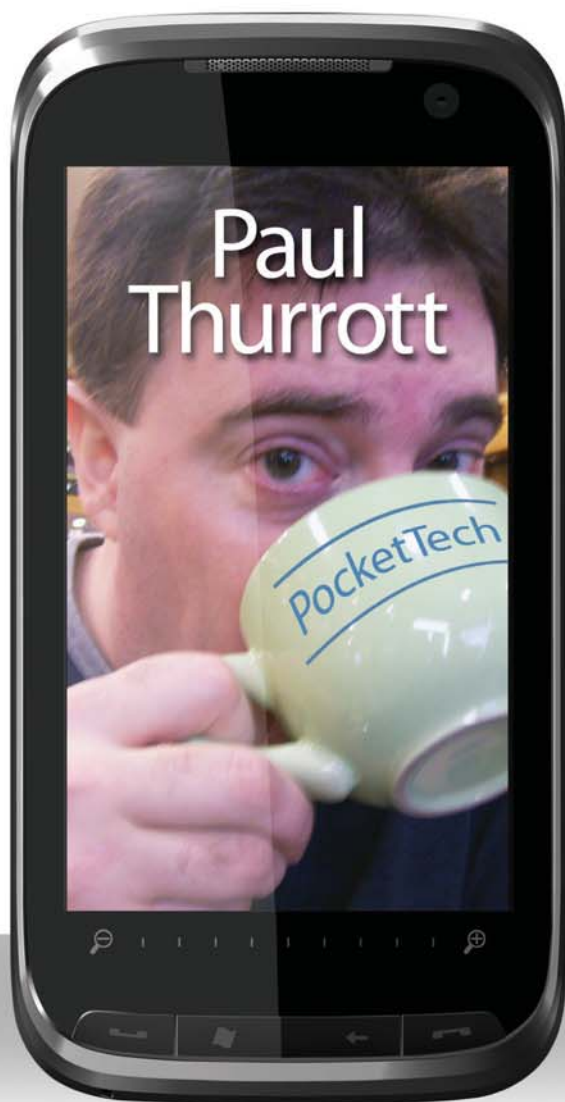
Since 2009, over 1,000 clients have moved business to IBM Power Systems™ from Oracle/Sun. Some were swayed by the up to 60% drop in IT costs. Others by the 3x per core performance (per both TPC-C and SAP SD benchmarks). And some by both. Though all saw the strong business case for moving. We'd welcome the opportunity to show how IBM could help your organization, too.

ibm.com/facts



IT COSTS: All client examples cited or described are presented as illustrations of the manner in which some clients have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual client configurations and conditions. PERFORMANCE: www.tpc.org as of 3/28/11 (IBM Power 780 (3 x 64 C)/24 C/192 C/768 Th; 10,366,254 tpmC; \$138/tpmC; avail 10/13/10 v Oracle SPARC SuperCluster w/13-4 Servers (27 x 64 C)/108 C/1728 C/13824 Th; 30,249,688 tpmC; \$101/tpmC; avail 6/1/11). TPC-C is a trademark of Transaction Performance Processing Council. www.sap.com/solutions/benchmark/ as of 3/28/11 (IBM Power 795 (32 P/256 C/1024 Th; 126063 users/2-tier SAP ERP 6.0 pack4/AIX 7.1 + DB2 9.7; cert 2010046 v Oracle SPARC Enterprise Server M9000 (64 P/256 C/512 Th; 39100 users/2-tier SAP ERP 6.0/Solaris 10, Oracle 10g; cert 2008042). SAP is a registered trademark of SAP AG in Germany and several other countries. IBM, the IBM logo, ibm.com, DB2, Power Systems, Smarter Planet and the planet icon are trademarks of International Business Machines Corp. registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml. © International Business Machines Corporation 2011.

Paul Thurrott...



... he's not in
Microsoft's pocket,
but now he can
be in yours.

The independent voice
for IT enthusiasts

Paul Thurrott delivers news, tips, commentaries, and reviews on Microsoft technology – from gaming to mobile to servers to software, and coverage of Microsoft competitors in between. Get daily updates without reaching farther than your pocket.

Download your
Paul Thurrott: PocketTech app today
winsupersite.com/go/app

Available for iPhone | Windows Phone 7 | Android





“Sometimes, wipe-and-reimage isn’t enough: The OS might be there—it just can’t boot.”

Fix Unbootable Systems with Bootsect

Target the MBR and what I call the WBR in your troubleshooting efforts

In “Adding Windows PE to Your Windows 7 System” (InstantDoc ID 129793), I showed you how to install an “onboard emergency kit” for repairing a non-booting system. But sometimes that kind of wipe-and-reimage process isn’t enough: The OS might be there—it just can’t boot. In that case, understanding the Windows boot process and some relevant boot-repair tools can save the day. (This is also a perfect way to build bootable systems from the ground up, which is why I’m continuing this short detour from the SteadyState stuff I’ve been writing about.)

Upon startup, your system first looks in its BIOS data for the order of devices to try when booting, so if you’re having problems, check the BIOS boot order first. (Hey, sometimes the easy answer is the right one!) A bootable disk also needs a sector called the Master Boot Record (MBR), which contains a bit of code (more on this later) and a table that contains the locations of the disk’s partitions. The BIOS loads both code and table into RAM, then executes the code. If the code is damaged (or just zeroes), the code execution will either bluescreen or hang the system.

To restore the MBR’s code portion, you can use Bootsect (bootsect.exe), a repair tool that Windows provides only in Windows PE and not in Windows 7/R2. Bootsect’s syntax looks like

```
bootsect /nt60 driveletter: /mbr
```

Its syntax is a bit convoluted, because drive letters (i.e., partitions, volumes) don’t have MBRs—physical disks do. Instead of letting you specify a physical drive number, however, Bootsect takes the drive letter, determines the physical drive it’s on, and restores the MBR code on that physical drive. For example, suppose I’ve booted WinPE and I have an external drive attached to my system—a drive that shows up as drive G. Suppose also that as far as my system is concerned, that external drive is physical drive number 5. To instruct Bootsect to rewrite its MBR, I’d type

```
bootsect /nt60 G: /mbr
```

And Bootsect would respond with something like

```
\\??\PhysicalDrive5
Successfully updated disk bootcode.
Bootcode was successfully updated on at least one volume.
```

Thus, Bootsect has determined that G is on drive 5, and it fixed drive 5’s MBR code. I’ve referred to the MBR code a couple of

times because starting at the 446th byte of the 512-byte MBR is the partition table. That’s why Bootsect rewrites only the code part; if it were to make your disk forget where your partitions were, it would essentially erase your hard disk (and your client would probably erase your invoice).

Once your PC has loaded the MBR, it executes that MBR’s code. That code has three jobs: Figure out which partition is “active” (i.e., bootable), load that partition’s first sector into RAM, and instruct the CPU to execute what ends up in RAM.

Let’s call that first sector of the active partition the Windows Boot Record (WBR). Like the MBR, it’s a small 512-byte space. Its code finds, loads, and executes a file named Ntldr (in Windows NT 3.1 through Windows Server 2003 R2) or Bootmgr (in Windows Server 2008, Windows 7, and Windows Vista). It’s a simple job, but—again—if the WBR becomes corrupted, your system will hang or bluescreen. Bootsect can fix a broken WBR in that case. So, again, boot WinPE and type

```
bootsect /nt60 driveletter:
```

For most systems, that drive letter is C when booted from WinPE. If you have a USB device that should boot but doesn’t, Bootsect /nt60 is often the answer. By the way, this command is why the /mbr option is so obtusely designed, as Bootsect has been around since Windows XP but got the /mbr option only recently. Clearly, in the retrofitting, the author wanted to save a bit of coding—thus, the volume-letter-points-to-drive-number circumlocution.

The WBR next loads Bootmgr, leading to the next item on our make-it-boot checklist: Is there indeed a file named Bootmgr on C? While you’re in WinPE, make that determination, and remember to ask to see hidden files:

```
dir c:\bootmgr /ah
```

If it’s not, just grab a copy of it either from the WinPE boot device or any copy of Windows 7/R2.

Next month, I’ll move to the next step: the BCD. (If you can’t wait for a working version of my SteadyState replacement, visit www.minasi.com to see all these concepts in action.)



InstantDoc ID 135806

MARK MINASI (www.minasi.com/gethelp) is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of 25 books, including *Administering Windows Vista Security: The Big Surprises* (Sybex).

Top 10 Free Tools for System Administrators

Audit Active Directory and file servers, detect inactive users, block USB devices, and more – for free

The following freeware tools by Windows IT Pro Community Choice Award Winner NetWrix Corporation can save you a lot of time and make your network more efficient – at absolutely no cost. All of these tools also have advanced commercial editions with additional features, but the freeware editions will not expire and will not stop working when you urgently need them.

1. Active Directory Change Reporter (Windows IT Pro Sep'09: InstantDoc ID 102446, TechRepublic: www.tinyurl.com/3lfo8qp)—This simple auditing tool keeps tabs on what's going on inside your Active Directory. The Windows IT Pro 2010 Community Choice and Editors' Best Award-winner tracks changes to users, groups, OUs, and all other types of AD objects, sending detailed daily reports with lists of changes. Download link: www.tinyurl.com/3jskosx

2. Privileged Account Manager (SC Magazine: www.tinyurl.com/3vsxskc) —This product maintains a repository of privileged user accounts (such as Administrator, root, service accounts etc) in Active Directory, servers, and other systems, providing a secure web-based portal for role-based access and automatic maintenance of shared administrative user accounts. The Privileged Account Manager can automatically generate strong passwords at specified intervals (e.g. every 30 days) and synchronize password changes on all target systems (for example, change service account password in Active Directory and update service credentials). Download link: www.tinyurl.com/3skae2d

3. USB Blocker (Windows IT Pro Nov'09: InstantDoc ID 102860)—The increasing mobility of flash drives, MP3 players, cell phones and iPods makes the threat of data theft greater than ever, and with a couple clicks of the mouse, this aptly-named tool blocks unauthorized usage of removable media via USB ports. USB Blocker hardens end point security by preventing the spread of harmful malware and restricting the transfer of confidential information. Download link: www.tinyurl.com/3pxk8fj

4. Password Expiration Notifier (Redmond Magazine Feb'09, 4sysops: www.tinyurl.com/3pr6eye)—This tool automatically reminds users to change their passwords before they expire, helping helpdesk administrators safe from password reset calls. It works nicely for users who don't log on interactively and, thus, never receive standard password change reminders at log on time (VPN and OWA). Download link: www.tinyurl.com/3huokq2

5. Inactive Users Tracker (MS TechNet Magazine May'08: www.tinyurl.com/44x4n5z, TechRepublic: www.tinyurl.com/3otxthk)—This tool tracks down inactive user accounts (e.g., terminated employees) so you can easily disable them, or even remove them entirely, thus eliminating potential security holes. The tool sends reports on a regular schedule, showing what accounts have been inactive for a configurable period of time (e.g., 2 months). Download link: www.tinyurl.com/3d5u5x2

6. File Server Change Reporter (4sysops.com: www.tinyurl.com/3hlvm5n)—This is a must-have tool for auditing file servers and appliances. The tool detects changes made to files, folders and permissions, and tracks newly created and deleted files. The tool is useful for detecting mistakenly deleted files and it allows quick backup recovery of accidental changes. Download link: www.tinyurl.com/3txsff

7. Active Directory Object Restore Wizard (Windows IT Pro: www.tinyurl.com/3rymxbq)—This tool can save the day if someone accidentally (or intentionally) deleted important Active Directory objects. It provides granular object-level, and even attribute-level restore capabilities that allow quick rollbacks of unwanted changes (e.g., mistakenly deleted users, modified group memberships, etc). Download link: www.tinyurl.com/3shavbm

8. VMware Change Reporter (TechTarget/SearchVirtualDesktop: www.tinyurl.com/3jupssl) — If you don't know what is being changed by your colleagues in the VMware infrastructure, it's very easy to get lost and miss changes that can affect the things for which you are responsible. This tool tracks and reports configuration changes in VMware Virtual Center settings and permissions. Download link: www.tinyurl.com/3hddx93

9. Windows Service Monitor (WindowsReference.com: www.tinyurl.com/3evpamh)—This very simple monitoring tool alerts you when some Windows service accidentally stops on one of your servers. The 2010 Windows IT Pro Community Choice and Editor's Best Award-winning tool also detects services that fail to start at boot time, which can happen, for example, with Microsoft Exchange. Download link: www.tinyurl.com/3ztclrc

10. Disk Space Monitor (MS TechNet Magazine Sep'09: www.tinyurl.com/3d3wan6)— Even with today's terabyte-large hard drives, server disk space tends to run out quickly and unexpectedly. This simple monitoring tool will send you daily reports regarding all servers that are running low on disk space, below the configurable threshold. Download link: www.tinyurl.com/42yaqzt



"CSVs and live migration were introduced with Server 2008 R2 and virtually every example of live migration uses CSVs."

Cluster Shared Volume FAQs

Get answers about storage, network requirements, live migration, and other details about CSVs

Cluster Shared Volumes (CSVs) are a new feature in Windows Server 2008 R2 that lets multiple cluster nodes concurrently access shared storage. In previous releases, only one node could host a virtual machine (VM) and access the Microsoft Virtual Hard Disk (VHD) files residing on the shared storage. CSVs can be accessed by all nodes of a failover cluster. This ability lets you create multiple VMs on the same LUN, and they can be accessed by multiple hosts. In this column, I'll answer 10 of the frequently asked questions about CSVs.

without CSVs, you need a separate LUN for each VM that will take part in the move. However, CSVs make live migration faster because there's no need to mount the new storage.

6 Are you limited to a single CSV per host?—No. By default, Windows Failover Clustering creates a single CSV mount point of C:\ClusterStorage\Volume1, but you're not restricted to using just that mount point, nor are you restricted to using that naming convention. You can create multiple CSVs and each must have a unique name.

7 How do CSVs appear to the host OS?—To the physical host system, the CSV is seen as a mount point in the standard file system. When you create a new CSV, the Failover Cluster Manager creates a folder for the CSV, which, by default, is found in the host's file system as C:\ClusterStorage\Volume1. If you create additional CSVs, they'll have different host folder names.

8 If you create a CSV, do you have to use it for all your Hyper-V VMs?—No. Using CSVs for your VMs is strictly optional. When you create a new VM by using the Hyper-V Manager or Virtual Machine Manager 2008, you have the option of storing its files on a CSV or on any other location that's accessible to the host.

9 How do CSVs appear to the guest OS?—To the VM guest, the CSV storage appears as standard storage. In other words, if the guest is created on a CSV and that guest is configured to use a single drive, the CSV storage simply appears to the guest as a C drive.

10 Are there any limitations to using CSVs?—Yes. CSVs are essentially like other host storage. However, CSVs don't support pass-through disks, which could be a significant limitation for some I/O intensive applications where pass-through disks can provide slight advantages in raw I/O performance. In addition, backing up VMs with Windows Server Backup from the host requires restoration of the entire image. Other backup solutions, such as Microsoft System Center Data Protection Manager (DPM) 2010, provide more options.

InstantDoc ID 135873

MICHAEL OTEY (motey@windowsitpro.com) is senior technical director for *Windows IT Pro* and *SQL Server Magazine* and author of *Microsoft SQL Server 2008 New Features* (Osborne/McGraw-Hill).

1 Do CSVs require SAN storage or can they be implemented using DAS?—CSVs must be implemented using shared storage; they can't be implemented on DAS. CSVs can be created by using any of the shared storage technologies that are supported by Server 2008 R2: iSCSI, Fibre Channel, and Serial Attached SCSI (SAS). However, CSVs do require NTFS as the file system.

2 Do CSVs require Windows Failover Clustering?—Yes. CSVs are created by using Windows Failover Cluster Manager, and they must be created on shared storage that's visible to the failover cluster. Therefore, Windows Failover Clustering is a requirement for using CSVs.

3 Do CSVs have any special networking requirements?—No. CSVs and live migration work over standard Ethernet network connections. Microsoft recommends that VMs have one network connection for client systems that are accessing the resources on the VMs. Microsoft also recommends a dedicated network for CSVs and other live migration traffic. In addition, if you're using iSCSI storage, Microsoft recommends an additional dedicated network for iSCSI traffic.

4 When you perform a live migration, does the VM get moved to a different CSV?—No. Multiple cluster nodes can access a CSV simultaneously, so there's no need to move or mount the VM's VHD files when live migration moves the VM to a new host node. CSVs let the new host node immediately access the existing VHD files.

5 Are CSVs required for live migration?—No. CSVs and live migration were both introduced with Server 2008 R2 and virtually every example showing live migration uses CSVs, so it's easy to jump to that conclusion. To use live migration



Deuby

"The best way to learn a new technology is often to build up the environment to become familiar with its underpinnings."

First Steps in Federation

Working through AD Federation Services Labs

You've been reading about cloud computing, and how you can use identity federation to securely extend your internal identity systems to cloud service providers. You've been studying the dance of many steps that comprises claims-based authentication within federation. But it's not the same as doing it yourself.

How do you gain some hands-on experience with federation? In a Windows shop, one option is to spend time with the *AD FS 2.0 Step-by-Step and How To Guides* (<http://tinyurl.com/adfsguides>). I've been working through these guides recently; the experience highlights not only how little Active Directory Federation Services (AD FS) shares with AD but also how few AD FS skills the average AD administrator has.

In fact, about the only thing that AD FS shares with AD are the words *Active Directory*. AD FS is grouped with Active Directory Domain Services (AD DS) because—along with Forefront Identity Manager (FIM), Active Directory Certificate Services (AD CS), Active Directory Rights Management Services (AD RMS), and Active Directory Lightweight Directory Services (AD LDS, though everyone stills calls it ADAM)—it's an important component of Microsoft's overall identity and access management (IAM) portfolio. These products are listed as peers on the Windows Server 2008 R2 AD page, but if you think of your IAM strategy in layers, AD FS is built on top of AD DS and AD CS. Therefore, you should think of it as an additional skill set on top of these two technologies. This also means that if you've never gotten around to learning about how public key infrastructure (PKI) and certificates work, now's the time to get started.

Information about AD FS is scattered across a number of locations on the Microsoft website, so it's easy to get confused about where to start. An important point to remember is that you'll be working with AD FS 2.0 (code-named Geneva in beta, so you'll see a number of Geneva references), which is a major improvement from the original 1.0 version. The *AD FS 2.0 Step-by-Step and How To Guides* contain 12 guides. Some show you how to use AD FS with Microsoft Business Productivity Online Suite (BPOS)/Office 365, Windows Azure, and Microsoft SharePoint. A key tenet of federation is its ability to work with other federation products that use the standard Security Assertion Markup Language (SAML) protocol, so other guides show how to interoperate AD FS with

PingFederate, Shibboleth 2, CA Federation Manager, and IBM Tivoli Federated Manager.

The best place to get started is the second-from-last walkthrough, *Federated Document Collaboration Using Microsoft Office SharePoint Server 2007 and AD FS 2.0*. Although it's the most complicated lab—and certainly the most complicated lab setup—it's where you need to start so that you can work with all the moving parts of federated identity. There are two ways to approach this lab.

The first way is to build it up yourself. Just below the SharePoint step-by-step guide is the *How to Set Up the AD FS 2.0 VM Lab Environment for Federated Collaboration* guide, which helps you build the SharePoint lab environment. No trivial exercise, this 50-page document guides you precisely through building four virtual machines (VMs), two domains, and the associated services necessary (which I'll describe shortly). Get one sentence wrong, and you'll have to go back and fix it somewhere down

the line. It's time-consuming, and it requires licenses for Server 2008 R2, SharePoint 2007, SQL Server 2005 and 2008 R2, and Office Professional 2007. However, the best way to learn a new technology is often to build up the environment to become familiar with its under-

pinnings. (I've posted an annotated PDF version of this guide with the web version of this article at www.windowsitpro.com, InstantDoc ID 135813.)

The other way to approach this lab is hidden in the SharePoint walkthrough: Download preconfigured Hyper-V VMs. This method will save you a lot of time on the front end, allowing you to focus on testing the federation scenarios. Be aware, though, that you won't get the experience of actually installing AD FS, and because this preconfigured lab (and we're talking about four OS instances and four server products that require license keys) contains nothing but trial versions, once you set up the lab you need to take your test drive quickly before it pulls a *Mission Impossible* and self-destructs. (Tip: You can extend the life of the OS instances by running `Slmgr .vbs -rearm` from an administrative command prompt. Doing so will extend the evaluation period by 60 days.)

The SharePoint federation lab is a business-to-business (B2B) scenario between two pharmaceutical companies, Fabrikam and Contoso Pharmaceuticals, as Figure 1 shows. Fabrikam is a pharmaceutical supply company, and Contoso is a drug manufacturer.

If you've never gotten around to learning about how PKI works, now's the time to get started.

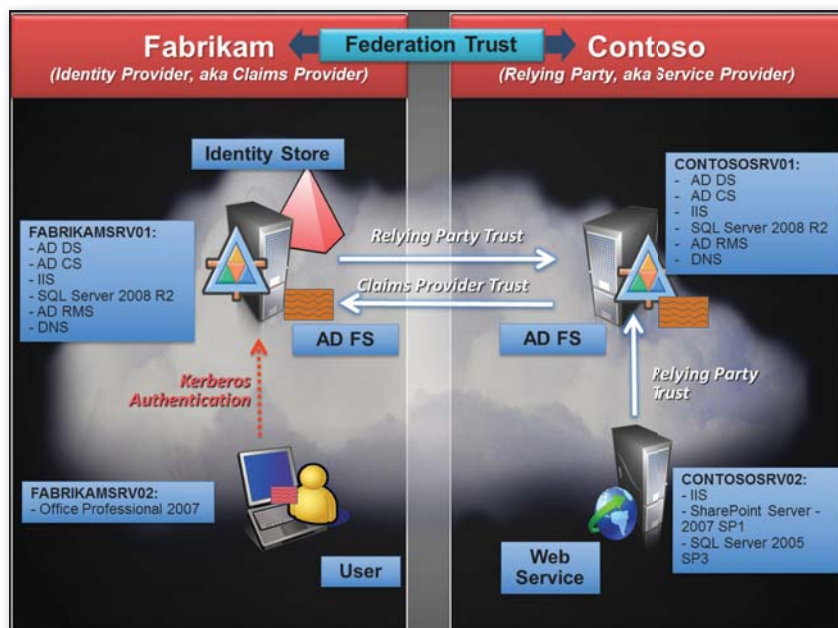


Figure 1: The SharePoint federation lab

Some Fabrikam employees need access to audit Contoso's drug-trial information, which is stored on a SharePoint 2007 service that's been made claims-aware with the installation of the Microsoft Federation Extensions for SharePoint. The lab shows how—by using AD FS to federate identities between Fabrikam and Contoso—Fabrikam drug-trial auditors can access the Contoso drug-trial documents on SharePoint without needing a separate account on Contoso.

To minimize confusion in often-complicated federation scenarios, I try to think of myself as being in the identity provider's role, and that role is always on the left side of the architecture diagram. Remember, the identity provider is the one that contains the identities (in this case, from AD) that will be extended to the service (in this case, Contoso's SharePoint server).

The SharePoint federation lab document is 96 pages long! And it's primarily made up of steps to take after you've either downloaded the VMs or gone through the 50-page lab-build document. The good news is that (unlike the lab-build document) the SharePoint document is made up primarily of screenshots. This makes the exercise much easier that it would have been otherwise, as in this case a picture really is worth a thousand words—and reduces tenfold the chance you might goof something up midway through the lab.

This lab is also easier than it might first appear because you don't have to go through the entire document if you want to just see how federation works. (Watching federation work, by the way, is hugely anticlimactic. Because it's single sign-on, federation is working correctly when, well, nothing happens. The cool part is that this "nothing" happens across security boundaries where something used to happen—like a credentials prompt—or you simply weren't able to connect to the remote resource at all.) The SharePoint lab contains 11 steps, but you only need to get through step 7 if you just want to watch federation in action.

If you've gone to all the trouble to get this far, however, you really should step through the rest of the lab. Step 8 shows how you can also use a SQL Server database as an attribute store that AD FS can access to generate claims. Step 9 shows how to configure AD FS and SharePoint to use AD RMS for digital rights management of documents. Finally, step 10 shows how to configure a second document library to use strong authentication to access its documents.

The two key VMs in this lab are FABRIKAMSRV01 and CONTOSOSRV01. They fulfill multiple roles for the lab, whereas FABRIKAMSRV02 is essentially an Office 2007 user (though it's installed on a server) and CONTOSOSRV02 is a SharePoint server (which requires IIS and SQL Server as components). First, FABRIKAMSRV01 and

CONTOSOSRV01 provide domain services through AD DS to create the FABRIKAM and CONTOSO domains. Note that because these lab domains have only one DC each, you don't have to worry about problems such as replication failing between DCs because the machines have been shut down, saved, or paused for greater than the tombstone lifetime. Second, they have DNS installed to support AD DS.

Third, both FABRIKAMSRV01 and CONTOSOSRV01 have AD FS installed. FABRIKAMSRV01's AD FS runs the claims provider STS (security token service—the service that generates SAML tokens) in this scenario. It's called the *claims provider* because it generates the claims necessary for SharePoint access from the user's AD attributes. Confusingly, STS is often used interchangeably with *federation server* or *AD FS*. CONTOSOSRV01's AD FS runs the relying-party STS—it relies on the claims coming from the claims provider.

Fourth, AD CS is also installed on FABRIKAMSRV01 and CONTOSOSRV01. This service provides each domain with a certificate authority (CA), which will generate certificates to prove the authenticity of the claims that each domain's STS will issue. Finally, IIS is installed on each to support both AD CS and AD FS.

If you have any intention of keeping up to date with identity and its future direction, I recommend that you install and work through at least the AD FS SharePoint lab. It will show you the foundations on which AD FS is built, as well as a typical B2B scenario that you can use AD FS for. The lab also provides hands-on experience working with claims as they make their way from the identity provider's STS to the service provider's STS to the claims-aware application. Finally, it highlights the areas you need to brush up on, such as IIS or Certificate Services. Though it's an identity technology, federation in general and AD FS in particular isn't something you learn overnight. Get a head start on understanding this important identity component by getting started on this lab.

InstantDoc ID 135813

SEAN DEUBY (sean@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Magazine*, and former technical lead of Intel's core directory services team. He's been a directory services MVP since 2004.



Nair

"Unfortunately, the error messages don't always point to a specific root cause."

WHAT WOULD MICROSOFT SUPPORT DO?

Tips for Troubleshooting Remote Desktop Connection Problems

Try this handy checklist for targeting the most common causes

As a systems administrator, you've probably experienced a problem connecting to a system via the Remote Desktop Protocol (RDP). Error messages such as *Remote Desktop Disconnected* and *This client could not establish a connection to the remote computer* represent recurring problems that we see in Microsoft Product Support. Unfortunately, such error messages don't always point to a specific root cause. Based on our experience, we've put together a cheat sheet of the most common causes of these problems: misunderstood terminologies and settings, incorrect permissions and/or user rights, port assignment conflict, and mis-configured Group Policy or RDP-TCP settings in Remote Desktop Services configuration

Note that this isn't a comprehensive list of all the various types of problems you might be experiencing while attempting to connect to a remote computer; they're merely the most common. The goal is to help you identify these problems before calling the Microsoft support team or hitting the search engine.

Misunderstandings

A common RDP misconception is that you need to install a Remote Desktop Licensing Server (aka Terminal Services Licensing) or Remote Desktop Session Host (aka Terminal Server) to allow remote connections. Out of the box, Remote Desktop supports two concurrent connections to remotely administer a computer. You don't need a licensing server for these connections.

Remote Desktop Licensing (RD Licensing)—formerly Terminal Services Licensing (TS Licensing)—is a role service in the Remote Desktop Services server role included with Windows Server 2008 R2. RD Licensing manages the Remote Desktop Services client access licenses (RDS CALs) that are required for each device or user to connect to a Remote Desktop Session Host (RD Session Host) server. You use Remote Desktop Licensing Manager (RD Licensing Manager) to install, issue, and track the availability of RDS CALs on a Remote Desktop license server.

Suppose you have three administrators in your IT team. You build a brand-new Windows Server system to serve as your new application server. To help with the initial settings, you have two admins remotely connected to this server (no licenses installed). When you have a change of shift, while one of the admins leaves work, the third admin tries to remotely connect to the same box. He sees that there are already two admins connected to the box, and if necessary he can force-disconnect one of them.

Also, remember that to allow remote connections for administrative purposes only, you don't have to install Remote Desktop Session Host (aka Terminal Server). Instead, ensure that the Remote Desktop setting is enabled in System Properties.

Another common misunderstanding involves knowing what permissions are needed to allow a user to log on to a remote computer. Members of the Administrators group don't need special permissions and can remotely connect even if they aren't listed in the Remote Desktop Users group. The Remote Desktop Users group on an RD Session Host server is used to give users/groups permission to remotely connect to an RD Session Host server.

You can add users and groups to the Remote Desktop Users group by using the Microsoft Management Console (MMC) Local Users and Groups snap-in, by using the Active Directory Users and Computers snap-in (if the RD Session Host server is installed on a domain controller—DC), or by accessing the Remote tab in the System Properties dialog box on an RD Session Host server (as you see in Figure 2) Adding a user to the Remote Desktop Users group using one of these methods will provide the appropriate permissions for remotely accessing a box. Otherwise, the connection will be denied.

Permissions and User Rights

What happens behind the scenes? How does adding a user to the Remote Desktop Users group give them the appropriate user rights to remotely connect to a computer? User rights, as their name suggests, control who is authorized to log on to a computer and how they can log on. In this case, the *Allow log on through Remote Desktop Services* user right controls remote access to a server.

If you pull up the local security policy on a server (Start\Run\secpol.msc), you'll notice that, by default, the Remote Desktop Users is already added to the *Allow log on through Remote Desktop Services* user right. Adding users to the Remote Desktop Users group also gives them this right.

Installing the RD Session Host role service on an AD DC isn't recommended. Allowing users to run programs on a DC could create security risks and performance problems. If the RD Session

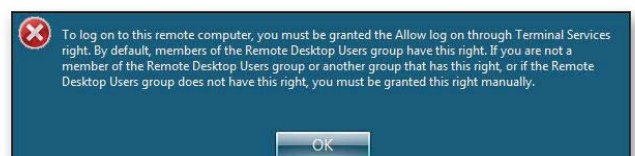


Figure 1: Missing membership to the Remote Desktop Users group

Host role service is installed on a DC, the security settings of the DC will need to be adjusted to allow users to have remote access to the server. This remote access is controlled by the *Allow log on through Remote Desktop Services* user right, which can be configured by using the Group Policy Management Console (GPMC).

On a DC, by default, only the Administrators group is granted the *Allow log on through Remote Desktop Services* user right. To allow remote access to the RD Session Host server for users who aren't members of the Administrators group, you should grant the Remote Desktop Users group the *Allow log on through Remote Desktop Services* user right.

Next time you see the error message that Figure 1 shows, be sure to check the Group Policy settings on the remote box. It's highly recommended that you don't add the user explicitly to the user right but instead follow the best practice of adding him or her to the Remote Desktop Users group and ensuring that the group isn't missing from the specific user right.

Port Assignments

Another common scenario is port blocking and/or port assignment conflict. To diagnose this problem, you not only want to check whether the default RDP port (3389) is blocked; you also want to make sure that it's being used by the appropriate service (TermService, in this case).

Here's a quick test that uses the Netstat and Tasklist commands, which you run on the server that you're trying to connect to remotely:

```
C:\Users\Administrator
.CONTOSOONE>netstat -a -o
```

```
Active Connections
Proto Local Address
```

```
Foreign Address State PID
TCP <IP address>:3389
<Server Name>:0 LISTENING 2252
```

The results show that the server is listening on port 3389. If port 3389 isn't listed, the server isn't listening on that port (possibly due to a host-based firewall or another ACL mechanism on the host machine that prevents the usage of that port).

But confirming that the port is open is only half of the battle. You still need to make sure that the right service is using that port. So, you grab the Process ID (PID) number from the results and run Tasklist to search for the string PID 2252.

```
C:\Users\Administrator
.CONTOSOONE>tasklist /svc | findstr
"2252"
```

```
Image Name PID Services
svchost.exe 2252 TermService
```

These results tell you that the port is being used by the right service (TermService, in this case). If you don't see the appropriate service listed, you can conclude that port 3389 is open (i.e., the server is listening on port 3389) but that another application is using it.

There could be legitimate reasons for reassigning the default RDP port to a different application, but then you need to determine which port is assigned to RDP. Note that Microsoft doesn't recommend changing the port assigned to RDP.

Misconfigured Settings

Another common scenario is where you're limited in the number of users who can connect simultaneously to a Remote Desktop session or Remote Desktop Services session. This scenario might come

in as a "failure to connect" Help desk call, and only after poking around a bit do you realize that although x users are able to connect, the $x + 1$ user fails with the error that Figure 2 shows. Note that these settings might also affect administrators who are trying to remotely administer a computer in the Remote Administration mode.

Two settings limit the number of Remote Desktop Services sessions that can be active on a server:

- **Limit Number of Connections**—You can use this Group Policy setting to restrict the number of remote sessions that can be active on a server. If this number is exceeded, additional users who try to connect receive an error message telling them that the server is busy and to try again later.
- **Network Adapter settings**—When you install the RD Session Host role service on the computer, the RDP-TCP connection is changed to allow an unlimited number of simultaneous remote connections. Note that if the *Maximum connections* option is selected and dimmed, the *Limit number of connections* Group Policy setting has been enabled and has been applied to the RD Session Host server.

Both of these settings help configure the number of simultaneous connections allowed for a connection. Restricting the number of simultaneous remote connections can improve performance because fewer sessions are demanding system resources. We often see admins enabling either of these settings to help improve performance today but not remembering it when they encounter a problem wherein only a few users are able to connect.

Resources

For more information, see the web version of this article (InstantDoc ID 135962) for a list of resources. Microsoft will regularly update these resources to reflect the latest developments.

InstantDoc ID 135962

SABIN NAIR (sabinn@microsoft.com) is a senior program manager in the Product Quality (PQ) group at Microsoft.



Figure 2: Reaching the simultaneous connection limit

READER TO READER

Mass Deploying "iThings"

The term *smartphone* doesn't mean the same thing it did just a few years ago. In the past, a phone that was smart could send and receive email, help you manage your appointments or tasks, and perhaps provide some basic applications, such as a calculator or games. Now, smartphones can be a complete OS platform, ready to complete any task that you program it to run. Many times, using the phone is an afterthought, as there are tens of thousands of applications (many of which are free) that can be installed on smartphones.

IT professionals need to start thinking about how these mini-computer platforms can help them do their jobs and better serve their customers.

This "ah ha" moment came to me recently when my employer, Eastern Washington University, purchased 20 Apple iPod touch devices for my staff. An iPod touch is basically an iPhone, minus the cellular capability. For less than \$230 a piece (and no recurring monthly charges), each technician received a tool that had wireless capability, could send and receive email, and had easy Internet browsing for researching problems. But that's just the start. We added a free application, Cisco Mobile 8.1, that turns iPods, iPhones, and iPads—aka "iThings"—into VoIP phones (with the proper back-end support). We also added a free application that lets us access tickets from the university's help desk tool, Web Help Desk. Finally, we added Text Now, a free texting application that Web Help Desk uses to alert technicians when they have a high priority ticket in the queue.



Eric B. Rux

In a nutshell, we created a very powerful tool for very little money, thanks to one of my top technicians, Kerwin, who came up with the idea. His forward thinking has saved the university thousands of dollars.

Just like deploying multiple PCs, deploying multiple iThings requires some additional planning and steps. Mass deployments can be broken into three stages:

1. Activation
2. Application deployment
3. Configuration

If you have a lot of devices (e.g., 100) to deploy, consider dedicating a computer (PC or Mac) for each stage. It can be helpful to place each computer on a large table.

The devices can then be passed from one table to the next in an assembly-line fashion. For 10 or 20 devices, you might want to use just one computer. You'll have to decide which method will be the most efficient for your environment.

Stage 1: Activation

Before you begin activating the iThings, I recommend you turn them on all at once. This saves you time because you won't have to wait for each one to boot up.

To activate each iThing, you need to connect it to a computer that's running iTunes, which you can download at www.apple.com/itunes. The activation is much easier and faster if iTunes is in activation-only mode. To enable this mode on a Windows computer, follow these steps:

1. Use Task Manager to verify that iTunes isn't running. If iTunes isn't completely shut down, the command given in step 2 won't work.

2. Open a command prompt window and run the command

```
"C:\Program Files\iTunes\iTunes.exe"
/setPrefInt StoreActivationMode 1
```

Although this command wraps here, you'd enter it all on one line. The same is true for the other commands that wrap.

Here are the steps to enable activation-only mode on a Mac OS X computer:

1. Use Activity Monitor to make sure iTunes isn't running.
2. Open Terminal and run the command

```
defaults write com.apple.iTunes
StoreActivationMode -integer 1
```

After iTunes is in activation-only mode, connect the first iThing to the computer. A message will appear noting that iTunes doesn't support syncing. This message appears because you turned off syncing when you enabled the activation-only mode. Click OK.

If everything is working correctly, the iThing should activate immediately. (There's no wizard to go through.) When you see a completion message, you can disconnect the device.

Repeat this procedure for the remaining iThings. After all the devices are activated, proceed to stage 2.

Stage 2: Application Deployment

To install the applications using iTunes, iTunes needs syncing support, so you first need to take iTunes out of activation-only mode. To disable this mode on a Windows computer, open a command prompt window and run the command

```
"C:\Program Files\iTunes\iTunes.exe"
/setPrefInt StoreActivationMode 0
```

To disable this mode on a Mac OS X computer, open Terminal and run the command

Tell the IT community about the free tools you use, your solutions to problems, or the discoveries you've made. Email your contributions to r2r@windowsitpro.com.

If we print your submission, you'll get \$100.

Submissions and listings are available online at www.windowsitpro.com. Enter the InstantDoc ID in the InstantDoc ID search box.

```
defaults delete com.apple.iTunes
StoreActivationMode
```

Next, download the desired applications from the iTunes Store using a generic company account that doesn't have a credit card associated with it. You can find instructions on how to do so at support.apple.com/kb/ht2534. Using a generic account is important because applications that are ghosted to other devices are permanently tied to this account, even if you log into iTunes on the device with your own account. This is a limitation of the Apple iOS that might be fixed in future releases.

Now, connect the first iThing to the computer and perform the following steps in iTunes:

1. Click Register Later.
2. Agree to the licensing terms and click Agree.
3. If prompted for the locator services, click Not Now.
4. Sync the applications to the device when prompted.
5. Arrange the application icons the way you want.
6. Sync one final time. You'll use this configuration to image the rest of the devices. You can think of this as your "master Ghost image."
7. Back up the device so that it can be restored to the other devices. Do this by



Figure 1: Sections in the Configuration Profile

clicking the device in iTunes while pressing the Ctrl key, then choosing Backup.

8. Clear the *Open iTunes when this <iThing> is connected* check box. This will prevent iTunes and the iPhone Configuration Utility from interfering with each other during stage 3.

9. Disconnect the device.

To deploy the applications to the remaining iThings, follow these steps:

1. Connect the device to the computer.
 2. Click Never Register or Register Later.
 3. Agree to the licensing terms and choose Continue.
 4. Choose *Restore from backup*.
- Note that if the device has already been provisioned, restore by clicking the device in iTunes while pressing the Ctrl key, then choosing Restore.
5. Clear the *Open iTunes when this <iThing> is connected* check box.
 6. Leave the device connected to the computer and iTunes while the device reboots so that it syncs one final time.
 7. Disconnect the device.

Stage 3: Configuration

In the last stage, you configure the iThings for your specific business needs by creating a Configuration Profile. You can think of the Configuration Profile as a Group Policy Object (GPO) for iThings. For example, you can create a Configuration Profile that:

- Requires users to enter a passcode. You can require users to create a passcode that's alphanumeric or a minimum length.
- Turns off the device after a specified number of seconds to save battery life and prevent unintended operation.
- Imposes media restrictions, such as not allowing movies or television shows.
- Allows synchronization with Microsoft Exchange Server and provides the settings (e.g., Exchange server address, domain) to do so.

To create the Configuration Profile, you need to use the iPhone Configuration Utility, which you can download for free from support.apple.com/kb/DL851. After you install the utility on your Windows or Mac OS X computer, click Configuration Profiles and configure each applicable section. You



Figure 2: Configuration Profile implementation

don't have to configure every section, as Figure 1 shows. For example, you can skip the VPN section if there are no VPN settings to configure. You can find detailed information on how to configure the sections in the "iPad in Business" web page at www.apple.com/ipad/business/integration.

After you're done configuring the profile, click Export. Leave the security set to *Sign configuration profile*. Save the profile with a name that identifies its purpose.

Next, connect one of the iThings to the computer. In the iPhone Configuration Utility, click the device's name under DEVICES. Choose the appropriate Configuration Profile and click Install. Disconnect the device. Repeat this procedure for the rest of the iThings.

At this point, the Configuration Profiles are installed on the devices but they haven't been implemented. Users must click Install on their devices (see Figure 2) and provide the requested information before the profile is actually implemented and enforced. For example, if the profile allows synchronization with Exchange, users are asked to provide their email address and password.

That's it. You've now successfully mass deployed multiple iThings. 

—Eric B. Rux, manager of technical support services, Eastern Washington University

InstantDoc ID 129961

■ Outlook 2010
■ Internet Explorer 8
■ VMware ESXi

■ Windows 7
■ SQL Server 2008

ANSWERS TO YOUR QUESTIONS

Q: How can Outlook 2010's status bar help customize my application?

A: Like many Windows applications, Microsoft Outlook has a status bar at the bottom of the main interface that provides certain information about the application. Outlook 2010's status bar is somewhat configurable.

To see the status bar configuration options in Outlook 2010, right-click the status bar at the bottom of the main Outlook window. The menu items have a check mark to toggle their presentation in the status bar on or off. The menu lists the following options in the order that they would appear in the status bar from left to right:

- Quota Information
- Filter
- Items in View
- Header Items in View
- Unread Items in View
- Reminders
- View Shortcuts
- Zoom
- Zoom Slider

Quota Information shows the amount of space left in the user's mailbox before the server-side quota is reached. The quota value displays only for MAPI accounts. The

Filter option indicates whether a filter has been applied to the current view. A text button labeled Filter Applied appears at the very left of the status bar; you can click this button to launch a new filter configuration window to customize the view. The three Items in View settings go together. Items in View reflects the total number of items in the folder. Unread Items in View is obviously the number of items that have yet to be opened, items marked as unread, and items not exposed to the reading pane for enough seconds to be considered read. The Unread Items in View value should always be equal to or less than the Items in View value.

If any outstanding Outlook meeting or appointment reminders haven't been cleared (by clicking Dismiss or Snooze when the reminder pop-up window appears), the number of reminders is also displayed in the status bar when enabled.

Shortcuts are represented by two buttons that quickly optimize the screen based on user activity. The options are Normal and Reading, which are identified on the status bar with one button for Normal screen layout beside another button that looks like an open book for Reading view. The Normal option switches the Outlook main view to a standard four-column view: navigation pane, Inbox list, reading pane, and to-do list. The Reading option snaps the view to maximize screen real estate for the reading pane and Inbox listing. The user can focus on reading message content with this view.

The Zoom slider magnifies content within the message body in the reading pane. The slider shrinks or magnifies content, text, and images anywhere from 10

Q: Can I slipstream Service Pack 1 (SP1) into my Windows 7 or Windows Server 2008 R2 image?

A: The installation of a service pack into an offline image of Windows 7 or Server 2008 R2 isn't possible because of changes made in Windows servicing starting with Windows Vista. Versions of Server 2008 R2 and Windows 7 with SP1 are available on MSDN and TechNet now.

If you have a custom image for your organization, you need to recreate it with SP1 installed. You can use something like the Microsoft Deployment Toolkit (MDT) or System Center Configuration Manager (SCCM) to create your images, which will automate the process and make it simple to recreate your corporate images when service packs are released.

—John Savill

InstantDoc ID 129755

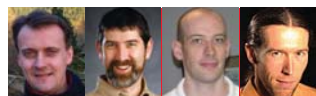
percent to 500 percent of their original size. If you have a scroll wheel on your mouse, you can use it to activate the zoom function. For messages with an embedded image that's just too small, you don't have to save the image and open it from an image editing application in order to magnify it.

Outlook 2010's status bar presentation options reside in the registry, at HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Outlook\StatusBar. These values are toggled between 1 for enabled and 0 for disabled. Because the registry values are read into memory when Outlook launches, you must restart Outlook for any changes to take effect.

Other Office applications also offer the status bar feature, but with options specific to the application. Outlook 2010's status bar displays only in the main Outlook window. If you double-click a message to open it in its own window, no status bar displays at the bottom of the window to provide context regarding the message.

—William Lefkovich

InstantDoc ID 129883



Jan De Clercq | jan.declercq@hp.com
William Lefkovich | william@mojavemediagroup.com
John Savill | jsavill@windowsitpro.com
Greg Shields | virtualgreg@concentratedtech.com

Q: What's the Active Directory (AD) Global Catalog (GC)-less logon feature? When can I use it and how do I configure it?

A: GC-less login is related to the universal group membership caching feature that Microsoft introduced in Windows Server 2003. It lets Windows 2003 and later domain controllers (DCs) cache a user's universal group memberships. To do so, it uses the msDS-Cached-Membership attribute of the user's AD user object. Universal group memberships are cached in this attribute the first time a user logs on. On subsequent logons by the same user, the DC uses the cached universal group memberships and doesn't have to contact a GC server. They're automatically refreshed every eight hours.

Universal group membership caching and GC-less login can be enabled at the AD site level from the NTDS Site Settings Properties of an AD site object in the AD Sites and Services MMC snap-in. You must select Enable Universal Group Membership.

Without GC-less login and universal group membership caching enabled, users always require access to a GC DC, because only GCs store the memberships of all universal groups in the Windows forest. GC-less login can be useful in small branch office site scenarios where you don't want to deploy a GC because of the extra WAN traffic that's generated to replicate the GC AD with other DCs. The need to contact a GC over a slow link at logon time can also be problematic and may result in branch office site users that are unable to log on to the domain if no GC is available.

The GC-less login feature doesn't completely take away the need to put a GC in every site—or at least to have one reachable GC for every site. Although GCs are no longer needed to find out about a user's universal group memberships, you still need them to resolve User Principal Names (UPNs—these are names of the format user@DNS_domainname) when your users log on using a UPN.

Also, if you still have Windows 2000 DCs, these DCs by default always require a GC DC to retrieve a user's universal group membership. This means that, by default, if no GC is available, a user can't

log on to a Windows 2000 DC. Microsoft provides a workaround for this Windows 2000 logon requirement—you can instruct a Windows 2000 DC to ignore GC failures. A GC failure occurs when no GC can be contacted to find out a user's universal group memberships at logon. This Windows 2000 workaround is based on the IgnoreGCFailures registry key (located in HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa). If a Windows 2000 domain consists of multiple DCs, this must be set on all DCs.

An annoying side effect is that the above registry change can create security holes when universal groups have been used to set permissions on resources in your Window forest. For example, if a user's universal group memberships aren't expanded, users could potentially access data on which a universal group they belong to was given explicit deny permissions.

—Jan De Clercq

InstantDoc ID 129842

Q: If I delete a Microsoft Application Virtualization (App-V) application from my machine, will I lose all of the application's settings when it's executed again?

A: Applications typically store information in your profile and in other areas of the file system and registry. Some changes made to your profile by virtualized applications persist as part of your standard profile, so deleting the virtualized application from your OS won't affect the settings. Other changes applications make are identified as user-specific during the sequencing of the application, such as a custom dictionary or toolbar changes in Microsoft Office, are stored in a separate package file on your machine that's unique for each virtualized application. This package isn't deleted when you delete a virtualized application from your machine, so customizations are maintained for when the application is executed again.

App-V creates a folder for each virtualized application that has custom changes under the %USERPROFILE%\AppData\Roaming\SoftGrid Client\application-GUID folder. For example, for my account and virtualized PowerPoint I see a folder named C:\

Users\john.SAVILLTECH\AppData\Roaming\SoftGrid Client\POWERPNT.V12-7F424220-BD7D-4D8C. Within this folder is a file that represents the stored changes that were captured by the virtualization engine that otherwise would have been written to the file system. You'll see a file, UsrVol_sftfs_v1.pkg, that represents all the user-specific data and configurations for the application. Note that because this package is stored under your roaming profile area, as long as you've enabled roaming profiles, the virtualized application settings will follow your user logon wherever you use the virtualized application.

If you want to delete your user-specific customizations and data for the application, instead of deleting the application within the App-V client, select Clear. The user-specific package file for the application will be recreated the next time you execute the virtualized application.

For more information about how App-V uses your disk space, check out the TechNet blog at tinyurl.com/3trqx8l.

—John Savill

InstantDoc ID 129932

Q: Multiple instances of Internet Explorer (IE) 8 or separate windows within IE seem to share cookies and now I can't use different logons in different windows. Why not?

A: There was a behavior change from IE 7 to IE 8 that allowed multiple browser windows and frames to share session cookies. This was done to create a seamless experience for users, so they don't have to re-enter credentials or data. However, in some cases users don't want the session cookies shared—they might want to connect to different sites with multiple Live IDs, or they might not want to share any data for security reasons.

Within IE's File menu (press the Alt key if it isn't visible), you can select a New Session option that will launch an IE instance with a different set of session cookies, allowing alternate credentials to be used.

Alternatively, you can add the -nomerge switch when launching iexplore.exe to start each IE window in its own session, with its own session cookies.

—John Savill

InstantDoc ID 129801

■ ASK THE EXPERTS

Q: I was using System Center Configuration Manager (SCCM) 2007 for software updates, but I've disabled it. How do I reset the clients to the Windows Update defaults?

A: When a client is configured to use SCCM 2007 for software updates, the policy of the machine is configured with the SCCM software update point as an intranet Microsoft update service location. To undo this, just use Group Policy to set that policy to Not Configured.

Navigate to Computer Configuration, Administrative Templates, Windows Components, Windows Update and set *Specify intranet Microsoft update service location* to Not Configured. Windows Update will use the Microsoft servers again.

—John Savill
InstantDoc ID 129894

Q: How can I book resources, such as a conference room, in Outlook 2010?

A: One of the features for scheduling meetings in Microsoft Outlook and Microsoft Exchange Server is the ability to book resources directly through Outlook's meeting request dialog. The Direct Booking feature uses logic coded in Outlook when adding Exchange mailboxes to a meeting request; this feature has been available since Outlook 2000. For MAPI connections to Exchange Server, Direct Booking occurs when the Exchange mailbox is added to a meeting request as a resource, the meeting organizer has the permission to write to the resource mailbox calendar, and the resource mailbox MAPI attribute `PR_PROCESS_MEETING_REQUESTS` is set to `TRUE`, which is the case when the mailbox is created as a resource mailbox in Exchange Server. If one of these requirements isn't met, the resource booking request is sent as it would be to any other Exchange mailbox—which means it will silently fail, because the request will remain pending in the resource mailbox Inbox.

In Exchange Server 2003, you need to deploy an Auto Accept event sink to automate responses from resource mailboxes. Since Exchange 2003, this logic is added when you create a resource mailbox. The

Direct Booking code is no longer necessary in the Outlook client.

You can still book resources directly in Outlook 2010; however, the feature is disabled by default. Unfortunately, Outlook 2010 doesn't prevent requests or warn users that resource room requests will fail. The meeting request is sent as though the resource will respond as a user does. Unless an administrator opens the resource mailbox and responds to the booking request manually, the request will remain pending with no response to the meeting organizer. The resource just doesn't get booked when you try to use Direct Booking. If you intend to use Direct Booking in Outlook 2010, you must enable it. To enable Direct Booking in Outlook 2010, you need to edit the `HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Outlook\Options\Calendar` registry entry.

Right-click in the open area in Regedit's right pane and select New, DWORD (32-bit) Value. Enter the value `EnableDirectBooking`, then double-click the new DWORD and assign it a value of 1 (1 is the same whether hexadecimal or decimal). This registry entry exists in Outlook 2007, Outlook 2003, Outlook 2002, and Outlook 2000, with the appropriate version number (14.0 for Outlook 2010, 12.0 for Outlook 2007, and 11.0 for Outlook 2003), and is set to 1 by default. If you want to disable Direct Booking in those versions of Outlook, reset the DWORD value `EnableDirectBooking` to 0.

If Outlook 2010 is open when you add this registry value, you'll need to restart Outlook for the change to take effect because the entry is read into memory as Outlook starts.

—William Lefkovich
InstantDoc ID 129884

Q: Where can I find the most common VMware ESXi log files?

A: Troubleshooting ESXi often requires digging through its text-based log files. You can use the `tail` command at the command prompt to see the last few lines for any log. The hard part, sometimes, can be finding where each log is stored. Here's a rundown on the location of ESXi's log files to aid your troubleshooting:

- `/var/log/messages`: Contains `VMkernel`, `vmkwarning`, and `hostd` logs.
- `/var/log/vmware/hostd.log`: Contains the Host Management services `hostd` log.
- `/var/log/vmware/vmware/vpx/vpxa.log`: Contains the VirtualCenter Agent log.
- `/var/log/sysboot.log`: Contains the system boot log.
- `/var/log/vmware/aam/vmware_hostname-xxx.log`: Contains the Automatic Availability Manager log.

—Greg Shields
InstantDoc ID 129659

Q: How can I set the minimum and maximum amount of memory SQL Server 2008 can use?

A: SQL Server 2008 will dynamically adjust how much memory it uses, but you can configure minimum and maximum amounts. The easiest way to set the minimum and maximum values is to use the SQL Server Management Studio (which is part of the SQL Server 2008 management tools installation option).

Right-click the database server and select Properties. Select the Memory page to expose the options to set minimum and maximum server memory (in MB). The smallest number that can be entered is 16MB, and the largest, which is set as default, is 2,147,483,647MB (2,048TB, or 2PB). You can set this to a more reasonable value for your environment based on sizing calculations.

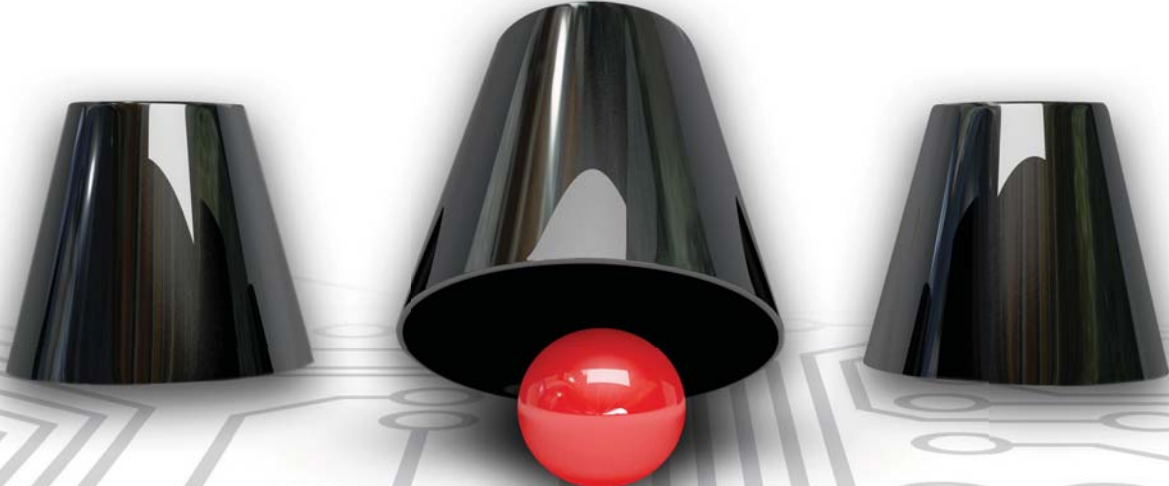
To change this setting using the SQL shell, you need to enable advanced options, then run the command

```
use master
EXEC sp_configure 'show advanced
options', 1
reconfigure
EXEC sp_configure 'max server memory
(MB)', 2048
```

To view the current value, just remove the `"2048"`. To set the minimum, set the `"min server memory (MB)"` value.

Changes take effect within a few seconds of setting the value and are reflected in the SQL Server memory performance counters.

—John Savill
InstantDoc ID 129797



Exchange Server Deployment Options

Several years ago, Microsoft used to ask, “Where do you want to go today?” as an advertisement for the Windows OS. Today, we can apply this same question to consider how we want to deploy Microsoft Exchange Server systems for our organizations. Several alternatives are available, including hosted email platforms, virtualized email platforms, and traditional on-premises physical hardware deployments—as well as various combinations of all these options. Because of the large number of available options, Microsoft’s old marketing question has never been more accurate than it is now. To choose the best deployment approach for your organization, you need to consider each option, including how all the options might be a good match (or a poor match) for the needs of your company.

Virtualized and
cloud-based
implementations

by Michael B. Smith

In this article, I explore some of the options for deploying Exchange Server, including the following:

- Installing Exchange Server on physical onsite servers—This option includes new decisions for Exchange Server 2010, such as continuing to use SAN storage, switching back to DAS, and determining the number of copies of data that are necessary.
- Virtualization—The ubiquitous deployment of virtualization for large and small solutions in the past 5 years has increased the benefits of Exchange Server virtualization, but challenges still exist.
- The cloud—Not a new concept, cloud deployment of Exchange has existed since at least Exchange Server 5.5.
- Hybrid environments—This approach combines local and cloud-based Exchange Server deployment.

The Traditional Choice

Exchange Server is considered the predominant business email system worldwide, with about 360 million seats deployed. Traditionally, Exchange is installed locally, on physical servers. Advantages of local Exchange deployment over virtualization and cloud-based solutions include the fact that no additional software is required, bare-metal processor and disk performance are available, and no additional Internet bandwidth is necessary.

No additional software. Exchange requires an OS, regardless of whether that OS is virtualized. However, whenever virtualization comes into play, some type of hypervisor (e.g., Microsoft Hyper-V, VMware ESXi, Citrix XenServer) is necessary to run the OS on the physical hardware. This extra software requires additional training, ongoing support, and maintenance, therefore adding to the overall

support burden and cost associated with maintaining an environment.

Cloud-based solutions often require several pieces of additional software, including software solutions that provide for single sign-on (SSO), so that users don't have to log on to each cloud-based solution separately; federation services, so that logon isn't required for cloud-based solutions; and Control Panel or other administrative software that provides systems administration. Some of these solutions might require installation on individual end-user workstations; other solutions might require their own servers and sets of specialized knowledge and administrators.

Improved processor performance. All hypervisors consume resources, which reduces the resources available to the OS image. Furthermore, a hypervisor is responsible for scheduling the resources available to the physical machine—and regardless of the number of virtual machines (VMs) present on a physical machine, the hypervisor always provides relatively small slices of processor time to each VM. This can cause the appearance of latency or jitter in a VM's operation, which is a major reason that virtualization isn't supported for many real-time or voice/video applications. In addition, the processor requirements of one VM can be so large as to affect the performance of other VMs. When combined, these problems can be reason enough to have dedicated physical servers assigned to certain workloads and applications.

Solutions that are based in the cloud have different performance requirements. The typical SSO application that's distributed to each end-user workstation has a negligible effect on the performance of an individual workstation. However, the infrastructure required to deploy and maintain that application can consume significant manpower. Federated services might also require additional local servers.

Improved disk performance. With the traditional approach, you don't have to worry about the overhead associated with disk drive virtualization. Modern hypervisors typically provide access to disk resources in three different formats: virtualized disk (VHD or VMDK formats), pass-through disk (assigning dedicated DAS and accessing that DAS without a virtualization

layer), and iSCSI/Fibre Channel (accessing remote block structured disk resources as if they were local). However, one of the key design characteristics associated with good Exchange performance is an appropriately designed disk subsystem—which holds true regardless of the deployment method.

In regards to cloud-based deployment, you depend on the company providing the hosted solution to design a disk subsystem that meets your needs, as well as the needs of all the other customers with whom you share hardware.

No additional Internet bandwidth.

When comparing a virtualized solution to the traditional solution, there's no expectation that the Internet bandwidth requirements differ between the two. Both the traditional and virtualized solutions are

solution. Therefore, except where differences exist, I don't mention those problems in this section. Some of the problems that I mentioned in the previous section might make you wonder why anyone would use virtualized resources at all. The answer is simple: high-performing hardware.

Processor performance that exceeds system requirements. Exchange Server was initially released requiring a processor with only a tiny percentage of a modern processor's power (a 66MHz 80486, for you history buffs). Granted, Exchange's feature content in those days, and the accompanying processor requirement for those features, was much less than today's—and we're fortunate that Moore's Law has provided us with multi-core processors that supply many times the level of performance required for most servers. This benefit can make it

Modern virtualization solutions depend on some deep concepts in OS kernel design and in the processor hardware itself, to ensure that one OS image can't adversely affect another.

generally designed and deployed presuming that most usage occurs locally and doesn't cross the LAN/WAN-to-Internet link.

But this isn't the case with cloud-based solutions. Instead, all communication between a company and the hosting provider occurs over the Internet. For some companies, this might mean that additional or redundant Internet bandwidth is necessary.

Virtualization

Modern virtualization solutions depend on some deep concepts in OS kernel design and in the processor hardware itself, to ensure that one OS image can't adversely affect another (and, in fact, can't affect it at all). This applies regardless of what the VMs might be executing—whether Exchange Server, Microsoft SQL Server, file and print services, etc. Each VM is protected from the code executing on all other machines.

In terms of cloud versus virtualization, the issues with the cloud are almost identical to the issues with the traditional

cost effective and resource effective to run many virtualized servers on top of a single physical server platform, even with the associated overhead of controlling those virtualized servers by the hypervisor.

This can mean that when running Exchange on physical hardware, the system might simply sit idle most of the time: consuming power, generating heat, but performing no useful activity. Although having growth potential and headroom is desirable, using resources efficiently via virtualization is even better.

Cheap memory. One thing that high-performing OSs like is memory. The more memory, the better! The initial version of Exchange Server required 32MB of RAM—a huge amount of RAM in 1996, but it supported 100 to 400 users per server. Today, an Exchange server requires a minimum of 4GB of RAM, and a multi-role server typically needs 12GB to 16GB of RAM to support 100 to 400 users.

Even low-end computers come with at least 2GB of RAM, with 3GB of RAM as

the standard for consumer-level 64-bit computers. At the enterprise level, 4GB or even 8GB of RAM is increasingly typical for the average workstation or laptop. High-powered laptops can often support 16GB of RAM.

On servers designed to support virtualization, 64GB or 128GB of RAM is common. Even for OS images of application products (such as Exchange Server and SQL Server) that demand a large amount of RAM, it can be very cost effective to combine multiple servers into one and still have more than enough memory to meet the needs of those applications.

Cheap disk storage. The price of storage is very specific to Exchange Server. In Exchange Server 2010 and Exchange Server 2007, the Exchange Server product team applied extensive engineering changes to optimize Exchange's behavior on slow and inexpensive disk. In fact, an array of slow 3TB 5,400rpm disks is quite capable of providing primary or archive mailbox storage for Exchange 2010. This type of slow disk is typically referred to as Just a Bunch of Disks (JBOD). Slow disk gives a great deal of flexibility to Exchange storage planners who intend to virtualize. It's entirely possible to use slow disk and achieve performance that can adequately support the load of hundreds, thousands, or even millions of mailboxes with Exchange 2010—given properly configured hardware.

However, using cheap disk has definite downsides. Cheap disk tends to fail more often (i.e., it has a lower mean time between failures—MTBF). A JBOD subsystem is designed differently than what a typical Exchange administrator is used to and usually requires additional monitoring. With the decreased MTBF of the disks, you need to have more spares on hand and be prepared to repair the subsystems more often, which might increase your costs.

You can use any of the following for an Exchange disk subsystem:

- Virtualized disk resources (VMDK or VHD files)
- RAID array(s) of DAS using slow disk
- RAID array(s) of iSCSI or Fibre Channel disk using slow disk
- Pass-through disk using slow disk

Of course, any of the following older solutions that use faster disk are also still available:

- Virtualized disk resources on fast disk
- RAID array(s) of DAS using fast disk
- RAID array(s) of iSCSI or Fibre Channel disk using fast disk
- Pass-through disk using fast disk
- SAN virtualized disk

Using cheap disk brings up a few caveats that you should be aware of. First, using slow disk is possible because of the tradeoff with memory utilization—that is, you shouldn't use slow disk and only the minimum memory for an application, because performance won't be ideal and in fact might not even be acceptable. Second, Microsoft supports using non-RAID solutions for mailbox storage (either a primary or archive mailbox), but only when at least three copies of the mailbox data exist across multiple servers (i.e., when using a database availability group—DAG—with a primary copy and a minimum of two secondary copies). If you don't have three copies of your data, for data safety and security reasons you should continue to use RAID-based solutions. Again, JBOD solutions require monitoring for each disk, as well as the awareness that these disks tend to fail more quickly than their more expensive counterparts. Finally, you can continue to use SAN disk storage or high-performance DAS, which might let you support more mailboxes per server than using JBOD. However, JBOD can provide excellent performance for the maximum recommended active mailboxes per Exchange server (4,000 to 5,000); therefore, using expensive disk isn't necessary for performance reasons—although companies such as NetApp and EMC offer solutions with very desirable features.

The cost of power. Each physical server consumes a certain amount of power. Typically, that amount of power is somewhat constant on a per-server basis. Of course, that's not strictly true—modern servers often can shut down underutilized processor cores, but when you compare, for example, three physical servers to a single physical server running three virtualized images, the server running the virtualized image will typically consume much less power. The power needs of a single server might not seem significant, but the heat generated by even a single server is noticeable. As more servers are added, the power

factor becomes more significant quite quickly, as does the amount of heat generated. Lower power requirements mean lower air-conditioning requirements—and therefore even lower power requirements.

Underutilized network resources. Today's typical network is much faster than networks only a few years ago. In the United States, 100Mbps to the desktop is common, and the switch fabrics in many server rooms are 1Gbps or even 10Gbps. Network virtualization is a mechanism for sharing network bandwidth among multiple VMs.

Other than backup applications, it's uncommon for today's networks to be fully utilized. Of course, this is a generalization—some companies do have heavily utilized networks, and it's quite possible to overcommit or saturate any network if either the physical or virtual networks are poorly designed.

In cases in which 1Gbps or 10Gbps isn't enough for a virtual server, because of hosting multiple VMs that require high network usage, hypervisors support assigning multiple virtual network cards (as well as multiple virtual network switches) to virtualized images. Network bandwidth that's available to the VMs is limited only by the number of card slots available to install physical NICs.

Hardware independence of VMs. Although I discussed some of the challenges associated with virtualizing hardware, I haven't yet covered the good part: hardware independence. When you build a VM, the NICs, CPU, IDE disk drives, etc., are all virtualized to a common set of hardware. That hardware is exactly the same regardless of whether you're running your hypervisor on the absolutely latest hardware or a server that you built 3 years ago. It's very easy to move a VM from one computer running Microsoft Hyper-V to another computer running Hyper-V or from one server running VMware ESX to another server running ESX. (Moving images between hypervisors is more challenging, but that's not what I'm talking about here.)

If you have a catastrophic failure on a server, restoring the VMs to operation is a simple matter of installing the hypervisor on another physical server and then restoring the server images from backup

(or from another cluster member). This is far simpler than rebuilding a server from a system state backup or any type of bare-metal backup. Simple restores from backup make great sense for Exchange roles that maintain little state information (e.g., a Hub Transport) or no state information (e.g., a Client Access server). However, a simple restore from backup isn't such a good idea for a Mailbox server that contains crucial data.

Infrastructure reduction. Combining many of the strategies that I discussed in this section obviously leads to having fewer physical servers. And fewer physical servers tends to reduce the number of physical switches, the number of physical racks, the amount of power, the amount of air-conditioning and air-handling systems, etc. These changes can make an operation more efficient and can help offset the costs that might be associated with switching to virtualization.

The Cloud

I admit that I'm a little tired of hearing about the cloud. The name is new, but the concept isn't—the cloud's basic functionality has been around for more than a decade. Of course, the cloud of today is more developed than the cloud of a decade ago. Ten years ago, you could do hosted Exchange. You could do hosted websites. You could do lots of things—individually. But few integration capabilities existed, and feature content was low.

Today, Microsoft's primary cloud offering is Business Productivity Online Standard Suite (BPOS), which includes hosted Exchange, hosted Microsoft Office SharePoint Server (Windows SharePoint Services—WSS, not Microsoft Office SharePoint Server—MOSS), hosted Live Meeting, and hosted Microsoft Office Communications Server (OCS). All these products have limited functionality when compared with their on-premises counterparts. However, at a cost of \$10 per month per user for the suite (US retail pricing), hosted applications can be very attractive to small businesses.

Microsoft is currently preparing its Office 365 offering, which might be available by the time you read this article. Office 365 will provide version upgrades to the BPOS product line, as well as significant additional feature content. Office 365

will add BlackBerry Enterprise Server (for free), Microsoft Office Web Apps, Exchange Server 2010 (upgraded from Exchange Server 2007), and Microsoft Lync 2010 (upgraded from OCS 2007). These features will provide IM and presence, the Lync Meeting replacement for Live Meeting, and PC-to-PC calling, as well as support audio, video, and desktop sharing. A full SharePoint 2010 installation is also included, rather than the limited WSS, which will let SharePoint-based organizations publish professional corporate public websites.

All of Office 365's solutions come with a much richer experience than BPOS in terms of command and control. Specifically from an Exchange perspective, Exchange 2010 adds configuration capabilities for both users and administrators within the Exchange Control Panel (ECP). The Office

A significant advantage to cloud-based mailbox servers is that you aren't subject to the whims of your local Internet provider as to whether email gets received for your company—at least as far as the destination email server—or whether email gets sent by your company (i.e., from the source email server). But if your local Internet provider is down, you can't access that email server, which makes that advantage somewhat moot. For geographically dispersed companies, having email in the cloud might remove access concerns for the "other" locations (i.e., the locations where the email servers weren't located previously). In that case, the remote locations are no longer dependent on the central location being available from the Internet. However, for many global companies, large or sufficient bandwidth already

The cloud concept isn't new—the cloud's basic functionality has been around for more than a decade, although the cloud of today is more developed than the cloud of a decade ago.

365 Control Panel goes even further: Many per-server and per-organization settings that were only previously available from PowerShell or Exchange Management Console (EMC) can now be executed from within the Office 365 Control Panel. With all of its added functionality and capabilities, Office 365 might become a real contender for replacing some onsite services with cloud-based services.

In most environments, implementing the solutions included as part of BPOS or Office 365 on premises will require a minimum of one server per application, an Active Directory (AD) infrastructure, a significant Internet connection, and software costs for the Windows servers, application servers, and CALs. A matching ROI could take a significant number of users or an extended period of time to achieve. However, for organizations that already have most of the requisite infrastructure, converting capital expenditure (CapEx) to a monthly operational expenditure (OpEx) might not be a reasonable choice.

exists between various facilities, so this configuration doesn't really represent an advantage.

Another potential advantage to cloud-based mailbox servers is that the local organization is no longer responsible for backup or recovery—those operations become the responsibility of the hosting company. However, this setup introduces significant complexity into the decision making process. First, an organization must consider whether the hosting company's backup and recovery options meet the organization's legal and corporate policy needs. Organizations are subject to a variety of data content and retention requirements based on the type of business and the country in which they're located. These requirements include but aren't limited to retention policies, data searchability and discovery, cleaning data after a secure data spill, containment of information such as credit card and other Personally Identifiable Information (PII), and the physical location of data. Organizations must look

Learning Path

WINDOWS IT PRO RESOURCES:

"Going Virtual with Exchange 2010,"
InstantDoc ID 104653

"Moving Exchange to the Cloud, Part 1,"
InstantDoc ID 103110

"Moving Exchange to the Cloud, Part 2,"
InstantDoc ID 103285

"Deploying Database Availability Groups in Exchange
Server 2010," InstantDoc ID 103536

"Migrating from Exchange Server 2003 to Exchange
Server 2010," InstantDoc ID 104657

"Preparing to Deploy Exchange 2010,"
InstantDoc ID 103517

"Exchange 2010 SP1: More Than a Simple Upgrade,"
InstantDoc ID 125644

"Exchange Server's Client Access: An Introduction,"
InstantDoc ID 125061

"Exchange Server's Client Access: Deploying Your
Servers," InstantDoc ID 125347

closely at a hosting company's policies and capabilities.

The availability of the hosting company's services must also be carefully measured and monitored. Regardless of the promises from hosting companies, downtime does occur—it's inevitable. Your agreement should include specific availability requirements and consequences if those requirements aren't met. This type of agreement is typically known as a service level agreement (SLA) and should also include mechanisms for the escalation of issues, notification of problems, specific definitions of who owns the data located at the hosting company, and how it can be recovered in the case of any termination of services.

Of course, no job is complete until the paperwork is done. To ensure that your company is receiving the appropriate value for the money spent, the hosting company should provide detailed billing and reporting. Large organizations that contract for dedicated hosting services can also require regular audits of the hosting provider.

None of these hosting requirements are free. Small organizations might ignore these criteria, but medium and large

organizations can't afford to—the price is worth the guarantee of availability.

Hybrid Solutions

With Office 365, it's possible to have some capabilities in the cloud (off premises) and some capabilities on premises. In fact, using Active Directory Federation Services (ADFS) or Forefront Identity Manager (FIM) 2010, you can effectively extend your onsite AD into the cloud. For example, you can opt to have 80 percent of your Exchange mailboxes in the cloud and 20 percent of them on a local Exchange server. It's unlikely that such an advanced scenario will be the typical solution for a small-to-midsize business (SMB). But a hybrid on-premises and off-premises solution might be a desirable option for larger organizations, especially those looking to dedicated Office 365 solutions.

Of course, onsite and offsite aren't the only types of hybrid solutions available. It's also possible and quite common to virtualize some Exchange servers and not others. For example, to ensure that maximum performance is eked out of available disk subsystems, and to ensure that there's no jitter in your voicemail, you might put your Mailbox servers and Unified Messaging (UM) servers onto physical hardware but put your Hub Transport and Client Access servers onto virtualized servers.

The ultimate hybrid solution might combine all the options. For example, you could have local physical servers, local virtualized servers, and some services in the cloud.

The Best Solution

Which solution is best for your company? The answer depends on many things. To find the best solution for your environment, due diligence requires you to examine each consideration and assess its applicability to your organization.

The cloud can potentially reduce local infrastructure requirements, but it can also raise many questions or issues around data storage, data recovery, security, legal requirements, availability, reporting, and SLAs. It's impossible to make a concrete recommendation without knowledge of a particular company's requirements in these areas. Using cloud-based solutions makes a company extremely dependent

upon Internet access and availability—which is a crucial component of buy-in to any cloud solution.

Although virtualization can also potentially reduce local infrastructure requirements (but for different reasons than cloud solutions), virtualization adds a piece of software (i.e., the hypervisor) that must be learned, supported, and maintained on every physical server. Virtualization also requires a change in design paradigms and therefore isn't necessarily a solution for all server needs.

The traditional choice is the easiest one—the one we're all familiar with—but this choice can lead to gross inefficiencies, such as having multiple physical servers when only one would suffice. Traditionally, the decision between onsite and offsite has been primarily about control: You can control more of your installation's features with onsite solutions (although that gap is slowly shrinking).

Moving Toward the Future

Most companies already have experience with cloud-based services, which might include anti-spam and antivirus solutions, patch management solutions, etc. Even on an individual basis, many of us use the cloud. After all, what are cable television and land-line telephones except different kinds of clouds?

Some companies will always keep their solutions local, to meet the requirements of their business. Still, many small companies have jumped eagerly onto the cloud bandwagon for their Exchange deployments, and many medium and large organizations have already virtualized some or all of their Exchange infrastructure. Moving other services into the cloud seems to be a growing trend, even though progress toward the cloud is still slow and careful. We're still very early on the adoption curve, but more is certainly yet to come.

InstantDoc ID 135832



Michael B. Smith

(Michael@theessentialexchange.com) is an independent consultant and a Microsoft Exchange Server MVP. He's been using Exchange since version 5.0 and working with messaging applications since 1981. He has a blog at theessentialexchange.com.

SIMPLIFY

command of the data center with
the power of convergence.

HP Converged Infrastructure simplifies what's next in management with HP BladeSystem.

Complexity drains your resources, leaving less for innovation.

Get it under control with the HP BladeSystem integrated, centralized management solution—HP Insight Control. With HP BladeSystem c7000 featuring the HP ProLiant BL460c G7 server powered by the Intel® Xeon® processor 5600 series, HP Insight Control can put you back in charge of your data center operations.

HP Insight Control delivers:

- Up to 40% increase in the productivity of system administrators*
- Up to 83% reduction in unplanned downtime*
- Payback in less than 5 months*

See how to take back control with the
IDC white paper *Gaining Business
Value and ROI with HP Insight
Control Management Software.*
>> hp.com/go/takecontrol4

HP ProLiant BL460c G7 server

- Two six-core Intel® Xeon® processor 5600 series (2.53GHz) installed
- 16GB of memory; expandable to 384GB
- HP Smart Array P410i Controller
- One integrated NC553i Dual Port 10Gb FlexFabric Converged Network Adapter
- Up to two HP hot plug small form factor SAS, SATA, or Solid State drives

\$4,759 (Save \$467)

Lease for just \$116 /mo.[†]

SmartBuy (PN: 630442-501)

*Source: IDC white paper sponsored by HP *Gaining Business Value and ROI with HP Insight Control Management Software*, #224704, September 2010

†Prices shown are HP Direct prices; reseller and retail prices may vary. Prices shown are subject to change and do not include applicable state and local taxes or shipping to recipient's address. Offers cannot be combined with any other offer or discount and are good while supplies last. All featured available offers in U.S. only. Savings based on HP published list price of configure-to-order equivalent (HP ProLiant BL460c G7 server, \$5,226 - \$467 = SmartBuy price \$4,759). Financing available through Hewlett-Packard Financial Services Company and its subsidiaries (HPFSC) to qualified commercial customers in the U.S. and is subject to credit approval and execution of standard HPFSC documentation. Prices shown are based on a lease 48 months in term with a fair market value purchase option at the end of the term and are valid through December 31, 2011. Other charges and restrictions may apply. HPFSC reserves the right to change or cancel this program at any time without notice.

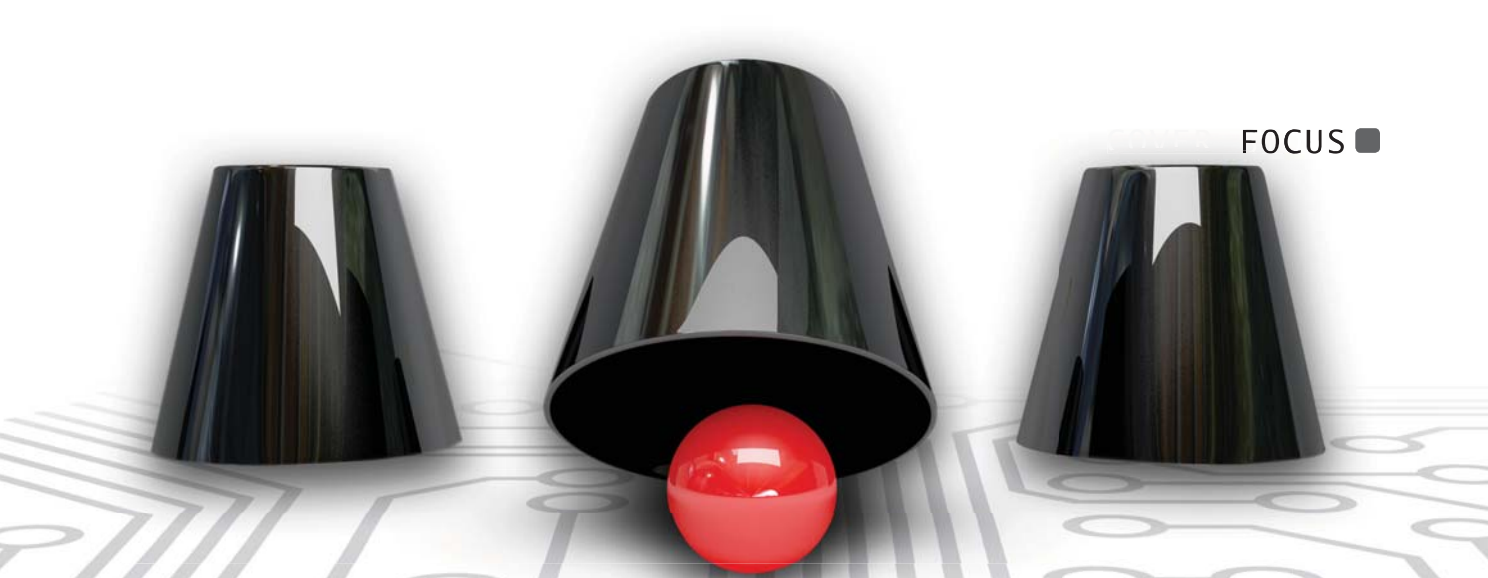
© 2011 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Intel, the Intel logo, Xeon, and Xeon Inside are trademarks or registered trademarks of Intel Corporation in the U.S. and other countries.



**Powerful.
Intelligent.**





Microsoft's Rajesh Jha Talks About the Future of Exchange

Recently, I spoke with Microsoft corporate vice president Rajesh Jha, who oversees the Exchange team, about what the future holds for Microsoft Exchange Server. Of course, much of this conversation focused on the role Exchange plays in Office 365 and the cloud, but Rajesh also had a lot to say about the importance of listening and responding to the requirements of customers and embracing changes in technology as a way to move the Exchange team forward.

BKW: As corporate vice president of Exchange Server, how much oversight do you have on Exchange Online? What's your role with the online side of things?

Rajesh: With Office 365, we had each of the core server engineering teams take accountability for the online version as well as the on-premises version. We believe this is exactly the right thing because the engineers who take our products to the enterprise, whether it be in the cloud or on premises or a combination, should be the same engineering team. That way, we can provide a seamless experience for our customers.

I have accountability for Exchange Server, Exchange Online, customers that might be in a hybrid mode. My peers here at Microsoft for Lync and SharePoint and the Office clients—they have the same model where they have accountability in the cloud and on-premises. This is a little different from the way we run the existing BPOS [Business Productivity Online Suite] services where we had a BPOS team that took our enterprise products and hosted them in a multi-tenanted environment for our customers. Going forward with Office 365, the engineering teams have both the servers and the service.

BKW: You hear a lot of numbers about how many Exchange mailboxes will be in the cloud versus on premises in 3 years, or 5 years. How much attention do you pay to statistics like that? Or is it the case that Microsoft is driving those numbers by the focus you're giving to putting Exchange in the cloud?

Rajesh: I'd say we don't really focus on the numbers. We focus on what our customers are telling us. And our customers have shown a lot of interest in moving to the cloud for a variety of reasons, whether it be flexibility, whether it be cost-savings, whether it be new features and new functionality. The customer interest is very much there. We believe the cloud is a very attractive proposition for many customers. But I'll be the first one to say that it's not going to be the solution for all our customers. We provide choice there.

BKW: What specifically do you think is driving the move to the cloud?

Flexible
deployment
options and
best-of-breed
experience
on any device
feature big in
the company's
plans

by B. K. Winstead

■ FUTURE OF EXCHANGE

Rajesh: For small and medium businesses, the cloud provides scalability of skills. For them, it's hard to attract and retain the right talent to keep their servers running at a high level of functionality and availability, go through the migration process, deployment process. In the cloud, we have Microsoft taking care of all of that for you. That's what I mean by scalability of skills. For some customers, it's just a cost savings. They get a modern experience, they get a modern infrastructure for collaborations and communications, and it's always up-to-date. They don't have the accountability of updating it—they focus on their business needs.

For large customers, it comes to both cost savings as well as flexibility. If you acquire another company, it's often more efficient to move these new employees to the cloud rather than to standardize an infrastructure across the new company. If I have deskless workers that haven't had email and I want to give them email, maybe I keep my existing infrastructure on premises and I choose the cloud to quickly provision my deskless workers with the new communications and collaborations.

For some customers, it's the new set of scenarios we've enabled with

Office 2010, Exchange 2010, SharePoint 2010, and Lync 2010. It's a complete communications and collaboration stack, and by moving to the cloud they're up-to-date with our latest stuff.



Rajesh Jha, Corporate Vice President for Microsoft Exchange Server

BKW: Give us your perfect vision of what Exchange Server will be in the future, whether that's in 5 years, or 10 years, or however far out you think about it.

Rajesh: I think the Exchange engineering team has always done a great job of listening to our customers. I'd like to take a tour into our history and use that to inform where we're going to go in the future. Exchange was the first product that built a modern web application with the Ajax programming model. We did that with Outlook Web App. Our ActiveSync protocol today is the de facto industry standard, and we invested in that because we heard from our customers that mobile access, anywhere access, was a big need. We've been invested in adding policies around ActiveSync because customers wanted manageability.

Fast forward to 2010, we've added a bunch of flexibility around storage options. Some customers continue to be on SANs, some want to get the cost savings from being on direct attached storage and JBODs. When I take a look at our work with Office 365, again, we're listening to our customers—they want choice, but they want the full enterprise platform. If you take just a simple example, look at our deployment record. We've updated that in the past few months after talking to customers who said, "Hey, make it easier for me to move from on prem to the cloud and stay in a hybrid mode." So we've added that capability through the deployment wizard.

I guess what I would say, when I think to the future, these attributes are going to continue to hold for the Exchange team. We want to listen to our customers. We want to give them flexibility. We want

to give them the best-of-breed experience on any device, anywhere access. We want to give them world-class manageability. And we want to make it

easy for their move to the cloud on their terms. These are the principles that will continue to inform our future investment.

BKW: Security remains a top concern for many businesses and IT pros, particularly for messaging. What steps is Microsoft taking with Exchange Online and with Exchange Server itself to address security problems?

Rajesh: Security and privacy, of course, are top considerations for any organization. With Exchange Server, we've talked in the past about soft controls and hard controls around security—controls, as in data protection. We have rules, a transport layer, that customers can customize to their specific needs. If they have certain sensitive information that they want not to leave their enterprise, they can put in rules to help with that. We have MailTips in our client, which is more in the realm of a soft control where we give people a quick reminder that perhaps they're mailing to somebody outside their organization, or their mail is going to a large distribution list. We have rights management capabilities that allow customers to restrict how mail gets forwarded around.

With Exchange Online, we are going through the most rigorous certification processes. We take a look at the way we operate the service, the way we protect customers' data, and that we have industry certification to give our customers that peace of mind. And then there are customers who, despite all of this, decide that it's too much of a leap for them to move to the cloud. They still have the option to run Exchange Server on premises, and they can run that in a way where perhaps the folks whose data they are most concerned about preserving stays on premises, and folks who feel they have less of an exposure can be in the cloud. It's not lost on any one of us that security is a prime consideration for our customers.

BKW: You mentioned going through online certification processes. Is that, for instance, the SAS 70? Can you talk about what's involved in these certification processes?

Rajesh: These certifications take a look at a lot of different aspects. Is the vendor good with patching their servers with security

updates, security patches? Are operational processes rigorous in terms of who has access to the data and how access is monitored and controlled? They look at the engineering processes that go into building a service. So it's pretty exhaustive. But for us, it's not enough just to go through the process—we want to go above and beyond that. So we're building capabilities into the product that go above and beyond just the certification process.

BKW: Mobile communications are on the rise everywhere. Are there particular challenges with Exchange Server that are cropping up as a result of additional mobile connections? What do you see happening in coming years as a result of increasing focus on mobile computing on smartphones and tablets?

Rajesh: I think the device proliferation is a real phenomenon. The average number of devices an information worker carries today is definitely not a single device. We all have our laptops, we might have a tablet, we might have a phone, we have our desktops. Ultimately, it's a really good thing because one of the principles that we have is that we should allow end users to get access to their information from wherever they are. We have so many mobile workers in our workforce. We have so many workers that are working in an office that's removed from the corporate headquarters. These workers want to get to their information, whether it be on a PC, the phone, or a browser on any platform.

So we're engineering to make all of that possible. OWA works on multiple browsers. Our Exchange ActiveSync stack has been implemented on pretty much any model of smartphone. There's a flip side to this, of course, which is to give IT admins the peace of mind that they can manage the devices, that they have a set of policies around these devices in terms of how they connect to the corporate data. So in the ActiveSync protocol, we've got those policies built in. I think this phenomenon is here to stay. People want access to their data on the go, whether it be in the browser or a rich device experience.

BKW: In some ways, Exchange is so mature, so well adopted, and so well understood that

it's really easy to talk about it. Of course, you never know what changes are just around the corner that might blow you out of the water—changes in technology, or the way people work, legal requirements, whatever. So you kind of hope change doesn't come and disrupt a good thing you've got going, but at the same time, you kind of hope it does because new things are always exciting.

Rajesh: I think we've had a lot of exciting changes in the industry. One of the things we've done with the Exchange team, we've embraced these changes. The cloud was a pretty big change. To take an enterprise product and take it to Internet scale was a substantial amount of engineering. We saw this coming 7 years ago. We didn't know it would be called the cloud. But in Exchange 2007, we reduced our I/O footprint by 70 percent on Exchange 2003. The reason we did that was we knew people would want large mailboxes. We were seeing the consumer cloud and the fact that the consumer cloud was setting expectations on large mailboxes. Then in Exchange 2010, we reduced the I/O by another 70 percent, so a 90-percent reduction over two releases. And that's what has allowed us to actually offer the giant mailboxes on Exchange Server.

That has been something that we spent a good part of the past 3 or 4 years engineering for. Getting coexistence to work where free/busy works whether the user is on prem or whether the user is in the cloud—they don't see the seams, they see one organization. It sounds for a minute like we think communications is a slow moving thing, but we think it's fast moving, and we're embracing it.

BKW: In a recent commentary, Paul Robichaux made predictions for messaging in the coming year ("Fearless Predictions for the 2011 Exchange Server World," InstantDoc ID 129424), and he wrote, "Microsoft corporate vice president Rajesh Jha, who owns responsibility for the Exchange team, will hold an arm-wrestling match with Gurdeep Singh Pall, the corporate vice president who owns the Lync team. The loser will have to turn his product into a server role for the winner's product, so we will either have Lync as a new Exchange role or vice versa." What do

you think about the possibility of Lync and Exchange merging?

Rajesh: That was funny. And I actually talked to Gurdeep and told him, "I'm pretty sure I'm going to win, Gurdeep." I was talking about the arm wrestling, of course. Gurdeep probably has a different point of view on that. I think what Paul talks about is really interesting. More than Exchange being a role of Lync or Lync being a role of Exchange, I think what he's talking about is that people expect their communications and collaboration and productivity stuff to interact better. With Office 365, of course we're going to have to do that.

Our customers don't see any of the back end. They should see one common manageability experience, one common licensing experience, one common user experience. We are absolutely working between Lync and Exchange and SharePoint and Office to make our servers be better integrated, the user experience be better integrated. With 2010, we've done a lot of work to make the whole be greater than the parts, and that's something we'll continue to do.

If Paul was talking about the fact that our customers don't expect silos of experiences, we get it. That's what we do in our office—we think about the experience across all of these different modalities.

BKW: And in the meantime, you're no doubt working on whatever the next version of Exchange will be?

Rajesh: I would just say: Of course. We are always working. Our engineers are working to make our existing products and services better. And they're working with customers to try and see what their needs are and what the industry trends are. So we're always at work.

BKW: Sounds exciting! Thanks, Rajesh. 

InstantDoc ID 129952



B. K. Winstead

(bwinstead@windowsitpro.com) is a senior associate editor for *Windows IT Pro*, *SQL Server Magazine*, and *SharePoint Pro*, specializing in messaging, mobility, and unified communications.

No Budget for Travel? No Problem!

Get the training you need right at your desk with

eLearning Courses

<http://elearning.left-brain.com>

Join industry experts for informative eLearning courses.

Each course includes in-depth sessions as well as live Q&A.

Our eLearning Series provides you with in-depth training on a variety of topics ranging from:

- ☐ Upgrading to SharePoint 2010
- ☐ Identity Management
- ☐ SQL Server for Non DBAs
- ☐ The Science of Great UI
- ☐ Administering SharePoint with Windows PowerShell
- ☐ And Much More!

Don't miss this opportunity for the training you need from the comfort of your own computer.

Check out the eLearning Series offerings today!

<http://elearning.left-brain.com>

THE CONVERSATION BEGINS HERE

COMING TO CHICAGO AUGUST 8-10, 2011!

SharePoint CONNECTIONS Coast to Coast TOUR + Microsoft® SharePoint BOOTCAMP

DIVE INTO SHAREPOINT 2010 WITH MICROSOFT AND SHAREPOINT INDUSTRY EXPERTS. SPEAKERS INCLUDE:

STEVE FOX MICROSOFT | ROBERT BOGUE THOR PROJECTS | DAN HOLME AVEPOINT

MICHAEL NOEL CONVERGENT COMPUTING | ASIF REHMANI SHAREPOINT-ELEARNING.COM | PAUL SCHAEFLEIN MINDSHARP

MATT MCDERMOTT ABLEBLUE | PAUL STUBBS MICROSOFT | DARRIN BISHOP APTILLON

AND MANY MORE! CHECK THE WEB SITE FOR THE FULL LIST OF SESSIONS AND SPEAKERS

The first 100 developers to register for the **SharePoint Coast-to-Coast Tour** get into the *Microsoft SharePoint 2010 Hands-On Development Bootcamp* for **FREE!**

**REGISTER EARLY
FOR ONLY \$499!**

TO REGISTER: DevConnections.com/SPTour 800.438.6720

COMING TO LAS VEGAS OCTOBER 31-NOVEMBER 3, 2011!

SharePoint CONNECTIONS

- Train with 100+ Microsoft & Industry Experts at over 240 deep dive sessions.
- Attend cutting edge keynotes & keep your competitive edge.
- Network with Microsoft, industry experts, and colleagues.
- Attend the co-located event sessions at no extra charge.

CHECK WEB SITE FOR DESCRIPTIONS OF SESSIONS AND WORKSHOPS

www.DevConnections.com 800.438.6720 • 203.400.6121

Keynote Speakers & Industry Experts



STEVE FOX
MICROSOFT



ANDREW CONNELL
CRITICAL PATH
TRAINING, LLC



SCOT HILLIER
SCOT HILLIER
TECHNICAL
SOLUTIONS



DAN HOLME
AVEPOINT



MICHAEL NOEL
CONVERGENT
COMPUTING



TED PATTISON
CRITICAL PATH
TRAINING, LLC

AND MANY MORE!

QUESTIONS ANSWERED • STRATEGY DEFINED • RELATIONSHIPS BUILT

Manage Network Drives with WSH Scripts

Use WshNetwork and FileSystemObject to list, map, and disconnect mapped drives

by Rob Gravelle

A Universal Naming Convention (UNC) path uniquely identifies a resource on a network. It describes the location of a volume, directory, or file, using the format `\\server\volume\directory\file`. However, most people prefer using a mapped Windows drive letter instead of a UNC path because a mapped drive letter is easier to remember. Therefore, your scripts will sometimes have to deal with mapped drives and mapped resources. It's at these times that you'll want to use the WshNetwork and FileSystemObject objects.

The WshNetwork and FileSystemObject objects are a dynamic duo when you need to work with mapped drives in Windows Script Host (WSH) scripts. Besides providing the same capabilities as Windows Management Instrumentation's (WMI's) Win32_MappedLogicalDisk class, the WshNetwork object has methods for creating and removing drive mappings. The FileSystemObject object provides methods for retrieving information about system drives. With the WshNetwork and FileSystemObject objects, you can easily perform a variety of mapping tasks, as the following examples demonstrate.

Determining Whether a Share Is Mapped

The IsDriveMapped function in Listing 1 demonstrates how you can use the WshNetwork object to determine whether a share is mapped. Here's how this function works. It first uses WshNetwork's EnumNetworkDrives method to return a list of the mapped network drives on a computer as a collection. This collection contains a pair of items for each mapped network drive: the drive's local name and its associated UNC path. The collection is zero-indexed so that the even-numbered items in the collection are the drive names and the odd-numbered items are the associated UNC paths. Therefore, the function iterates through every second item in the collection for comparison to the specified share. If there's a match, the function's return value is set to *true*. Otherwise, a value of Nothing is returned, which evaluates to *false* in Boolean comparisons.

To use the IsDriveMapped function in a script, you call it using code such as

```
If IsDriveMapped("\\Svr1\Electronic\") Then
    ' Do something.
```

or

```
If Not IsDriveMapped("W:") Then
    ' Create a new drive mapping.
```

Finding the Next Available Drive

Typically, you don't want to map a resource or share to an arbitrary drive letter. It makes more sense to find the next available one. Although the WshNetwork's object's EnumNetworkDrives method is great for listing mapped drives, it's not much help in finding available drives. A better approach is to use

Listing 1: IsDriveMapped Function

```
Function IsDriveMapped(strShare)
    Dim oNet, drv, i
    Set oNet = _
        CreateObject("WScript.Network")
    Set drv = oNet.EnumNetworkDrives
    For i = 0 To drv.Count - 1 Step 2
        If StrComp(drv(i + 1), strShare, _
            vbTextCompare) = 0 Then
            IsDriveMapped = true
            Exit For
        End If
    Next
End Function
```

Listing 2: GetNextDrive Function

```
Function GetNextDrive()
    Const A_DRIVE = 65, Z_DRIVE = 90
    Dim FSO, letter, drv
    Set FSO = CreateObject(
        "Scripting.FileSystemObject")
    For letter = A_DRIVE To Z_DRIVE
        drv = Chr(letter) & ":"
        If Not FSO.DriveExists(drv) Then
            GetNextDrive = drv
            Exit Function
        End If
    Next
End Function
```

the `FileSystemObject`'s `Drives` collection, as it contains information about both local and network drives in a system.

The `GetNextDrive` function in Listing 2 finds the next available drive. The function begins by enumerating the ASCII codes representing the possible drive letters. With this approach, the function's loop counter can easily convert the ASCII codes into drive letters by applying the `Chr()` function and appending a colon (:). For example, the ASCII code of 65, which represents the uppercase letter A, is transformed into A:.

`GetNextDrive` transforms one ASCII code at a time. Once transformed, the function uses the `FileSystemObject` object's `DriveExists` method to determine whether that drive already exists. The `DriveExists` method returns a value of *true* when the drive exists and a value of *false* when it doesn't exist. If the drive doesn't exist, the function's return value is set to that drive letter.

To use the `GetNextDrive` function, you need to customize the starting and ending loop indexes in the line

```
Const A_DRIVE = 65, Z_DRIVE = 90
```

so that they correspond to the available drive letter range in your system. For example, if the A and B drives are reserved for removable devices and the C drive is reserved for the first hard disk partition, you'd change this line to

```
Const D_DRIVE = 68, Z_DRIVE = 90
```

so that the function starts from the D drive. You can find a list of the ASCII codes at www.ascii-code.com.

You can use the `GetNextDrive` function in code such as

```
strDriveLetter = GetNextDrive()
```

```
If Not IsEmpty(strDriveLetter) Then
```

```
    Set objNetwork = _
        WScript.CreateObject(
            "WScript.Network")
    objNetwork.MapNetworkDrive _
        strDriveLetter, _
        "\\Svr1\Electronic\"
```

This code uses the `GetNextDrive` function to find the next available drive, then maps that drive's letter to the `\\Svr1\Electronic\` share. To map the drive, the code uses the `WshNetwork` object's `MapNetworkDrive` method, which I'll discuss shortly.

Disconnecting a Mapped Drive

You can use the `WshNetwork` object's `RemoveNetworkDrive` method to disconnect a mapped drive. This method has one mandatory and two optional arguments:

- **Name.** You use this mandatory string argument to specify the name of the mapped drive you want to disconnect. It can be either a local name or a
- **LocalName.** You use this mandatory string argument to specify the drive you want to map. If the name is a drive letter, you need to include the colon (e.g., G:).
- **RemoteName.** You use this mandatory string argument to specify

remote name, depending on how the drive is mapped.

- **Force.** You use this optional Boolean argument to disconnect the mapped drive, even if files are in use. Values are *true* and *false*.
- **UpdateProfile.** You use this optional Boolean argument to specify that you want to remove the mapping from the current user's profile. This argument might be used if the `RemoveNetworkDrive` method is part of a logon script, for example. Values are *true* and *false*.

For example, if you want to remove the Z drive mapping even if a resource is being accessed, you'd use the code

```
objNetwork.RemoveNetworkDrive("Z:", true)
```

Mapping a Network Drive

You can use the `WshNetwork` object's `MapNetworkDrive` method to map a drive letter to a shared folder or any child folder under a shared folder. `MapNetworkDrive` has two mandatory and three optional arguments:

- **LocalName.** You use this mandatory string argument to specify the drive you want to map. If the name is a drive letter, you need to include the colon (e.g., G:).
- **RemoteName.** You use this mandatory string argument to specify

Listing 3: MapNetworkDrive.vbs

```
Dim strLocalDrive, strRemoteShare, objNetwork
strLocalDrive = UCase(Left(WScript.Arguments.Item(0), 2))
strRemoteShare = WScript.Arguments.Item(1)
Set objNetwork = CreateObject("WScript.Network")

On Error Resume Next

objNetwork.MapNetworkDrive strLocalDrive, strRemoteShare, False

' Error traps
If Err <> 0 Then
    Select Case Err.Number
        ' Persistent connection so try a second time.
        Case -2147023694
            Err.Clear
            On Error Resume Next
            objNetwork.RemoveNetworkDrive strLocalDrive, True, True
            objNetwork.MapNetworkDrive strLocalDrive, strRemoteShare, False
            WScript.Echo "Second attempt to map drive " & _
                strLocalDrive & " to " & strRemoteShare
            ' The local drive letter (aka local device name) is already in use.
            Case -2147024811
                WScript.Echo "ERROR: Failed to map drive " & _
                    strLocalDrive & " to " & strRemoteShare & ". " & Err.Description
            Case Else
                WScript.Echo "ERROR: Failed to map drive " & _
                    strLocalDrive & " to " & strRemoteShare
    End Select
End If
```

■ MANAGE NETWORK DRIVES

the shared folder's UNC name (e.g., \\ServerName\ShareName, \\ServerName\ShareName\FolderName).

- **UpdateProfile.** You use this optional Boolean argument when you want to store the mapping information in the current user's profile. Values are *true* and *false*.
- **UserName.** You use this optional string argument when you want to map the network drive using the credentials of someone other than the current user.
- **Password.** You use this optional string argument to specify the password for the user identified by the **UserName** argument.

Many times you can map a drive using only the mandatory arguments. In administrative scripts, though, it might be necessary to supply an alternative or elevated set of credentials to successfully connect to a share because you can't map a drive to a folder unless you have permission to access that folder. After the connection is established, the supplied credentials

govern access to the network drive for the duration of the connection.

When using the `MapNetworkDrive` method, it's important to include some error-handling code because there are a few conditions that can cause it to fail. Common causes are insufficient permissions, the local drive letter is already in use, and a persistent connection (one that reconnects after a reboot or logout). For example, the `MapNetworkDrive.vbs` script in Listing 3 handles two types of errors: the local drive letter is already in use and a persistent connection already exists. The latter error condition isn't a fatal one, as you can still disconnect the drive for the current session using `RemoveNetworkDrive`.

To map the D drive to the remote share \\Svr1\Electronic\, you'd use

```
MapNetworkDrive.vbs
D: \\Svr1\Electronic\
```

By default, `MapNetworkDrive.vbs` doesn't update the current user's profile with the mapping information. If you want to update the current user's profile, you can change the line in callout A to

```
objNetwork.MapNetworkDrive _
    strLocalDrive, _
    strRemoteShare, True
```

Indispensible Tools

The `WshNetwork` and `FileSystemObject` objects are indispensable tools when you need to manage mapped drives and resources in WSH scripts. I've only covered a few examples of what you can do with them. You can explore other options in MSDN's `WshNetwork` Object page at [msdn.microsoft.com/en-us/library/s6wt333f\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/s6wt333f(v=VS.85).aspx) and in MSDN's `FileSystemObject` Object page at [msdn.microsoft.com/en-us/library/6kxy1a51\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/6kxy1a51(v=VS.85).aspx).

InstantDoc ID 129966



Rob Gravelle

resides in Ottawa, Canada, and is the founder of GravelleConsulting.com. Rob has built systems for intelligence-related organizations such as Canada Border Services and for commercial businesses. In his spare time, Rob has become an accomplished guitar player and has released several CDs.

The cloud is changing how IT builds and delivers applications and services. Visit **CloudITPro** for the latest news, blogs and analysis to help you determine your organization's cloud strategy.

CloudITPro
CloudITProOnline.com

**2 new
sources
for next
generation
information**

GET THE eNEWSLETTERS:
CloudITProOnline.com
MobileDevProOnline.com

MobileDevPro
MobileDevProOnline.com

MobileDevPro bridges the gaps between the mobile industry, the IT and developer communities, and an increasingly mobile business world that seeks to understand the benefits of mobile technology.

BROUGHT TO
YOU BY:

WindowsITPro
DevPro

DirectAccess

Improvements in Forefront Unified Access Gateway SP1

DirectAccess is a breakthrough technology first released in Windows Server 2008 R2 and Windows 7 that gives remote users seamless access to the corporate network from anywhere on the Internet, without the need to manually connect to the corporate network. IPv6 and IPsec let organizations extend their network to any point in the world where Internet connectivity is available, thus improving users' productivity and experience.

Microsoft has released several improvements to DirectAccess since the technology's original release. DirectAccess server support was added to Microsoft Forefront Unified Access Gateway (UAG), with features that simplify deployment, such as IPv6-to-IPv4 translation (NAT64/DNS64) and support for scaling and high availability using server arrays. On the client side, a free DirectAccess Connectivity Assistant (DCA) tool was released that provides end-user notifications and client troubleshooting.

Microsoft has now released Forefront UAG SP1. In addition to fixing several bugs, Forefront UAG SP1 incorporates several improvements in DirectAccess support. These changes include "always managed" functionality, native support for Force Tunneling, one-time password (OTP) authentication, enhanced monitoring and logging capabilities, and easier deployment. With these improvements, DirectAccess is an even more appealing technology for enterprises than ever before.

"Always Managed" Functionality

Although much of the hype around DirectAccess has centered around users' transparent access to internal network resources, for many IT departments the most appealing aspect of DirectAccess is the ability to extend desktop management functions beyond corporate network boundaries. DirectAccess provides this functionality by using two different IPsec tunnels when connecting to the Forefront UAG DirectAccess server. The first tunnel, called the infrastructure tunnel, connects the machine to the domain controllers (DCs) and management servers. The infrastructure tunnel uses only machine credentials for authentication and remains connected as long as the machine has Internet connectivity. The second tunnel, called the intranet tunnel, uses both machine and user credentials to connect the user to the other servers on the internal network and is active only when the user logs on and tries to reach one of those servers.

Because the infrastructure tunnel is always connected, standard Windows features such as Group Policy settings and password changes, as well as management software such as antivirus, software distribution, and monitoring and compliance tools, can now transparently work from anywhere on the Internet. For example, an organization can push a new antivirus update or a critical patch down to all its computers and receive a report of the success of the operation without waiting for users to eventually connect their machines back to the corporate network, or without setting up an additional remote management infrastructure in a demilitarized zone (DMZ) network.

Better security,
simpler
deployment,
and easier
management

by Fernando Cima

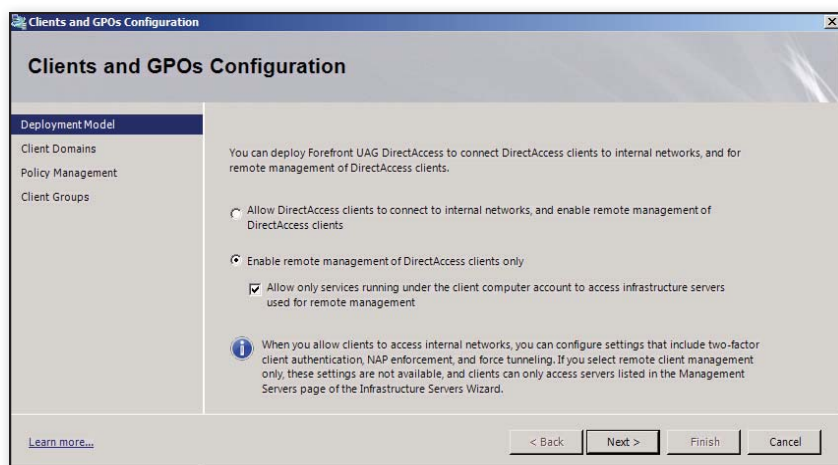


Figure 1: Selecting the management-only deployment scenario

Forefront UAG SP1 introduces support for an organization to deploy DirectAccess for remote management only, without actually providing end users access to the internal network. Machines can use DirectAccess to access Active Directory (AD) and desktop management services, while end users continue to use their existing remote access technologies—such as VPNs or web publishing portals—to connect to internal resources.

In this “always managed” mode, which Figure 1 shows, clients are configured only with the IPsec infrastructure tunnel, with no intranet tunnel. This approach greatly simplifies DirectAccess deployment, because the scope of the deployment is narrowed to only the servers that will be exposed to external clients. DirectAccess becomes a powerful tool for IT departments to extend their management capabilities, such as transparently using Microsoft System Center Configuration Manager (SCCM) and AD Group Policy Objects (GPOs) with clients anywhere on the Internet, without immediately replacing the existing remote access technologies that end users already have in place to connect to the corporate network.

The infrastructure tunnel is established only with the IP addresses specified in the DirectAccess policy, allowing an organization to determine exactly which servers DirectAccess clients can reach. Forefront UAG SP1 can automatically discover AD DCs, as well as Network Access Protection (NAP) and SCCM servers, as Figure 2 shows. In addition, Forefront UAG SP1 provides an optional safeguard

to allow only service accounts to connect through the tunnel, blocking non-administrative users from connecting to these servers.

Because only management traffic goes through DirectAccess in this mode, a Forefront UAG SP1 server will likely support a lot more concurrent machines than a default DirectAccess deployment with end user connectivity. In a test conducted by the Forefront UAG product group (blogs.technet.com/b/edgeaccessblog/archive/2010/06/22/forefront-uag-directaccess-performance-information.aspx), a Forefront UAG server that supported 2,300 concurrent users in the default DirectAccess configuration was able to handle 4,000 concurrent users with DirectAccess in “always managed” mode. With easier deployment, better scalability, and no end-user impact, this approach can

be the best way for many organizations to take advantage of DirectAccess’s benefits.

Force Tunneling

On the opposite end of the spectrum, some organizations require that every communication from end users is routed through the corporate network, then back to the Internet if necessary. To address this requirement, Forefront UAG SP1 adds native support for the Force Tunneling option, which previously had to be configured separately through a Group Policy setting.

Split tunneling is enabled by default in DirectAccess. For those not familiar with the term, this means that the client sends traffic through its DirectAccess tunnels only to destinations in the internal network. Traffic to the Internet is delivered directly, without passing through the DirectAccess server. The same approach is used for DNS queries: Names in the internal DNS namespaces are sent for resolution by internal DNS servers, whereas names from other namespaces are resolved by the DNS server provided by the local network. Split tunneling typically provides the best user experience because it tends to use the most direct route to reach the destination, while reducing network and CPU consumption on the DirectAccess server.

However, many organizations are wary of using split tunneling because of security reasons. Some companies have policy or regulation requirements to inspect all traffic from the client, whereas others are

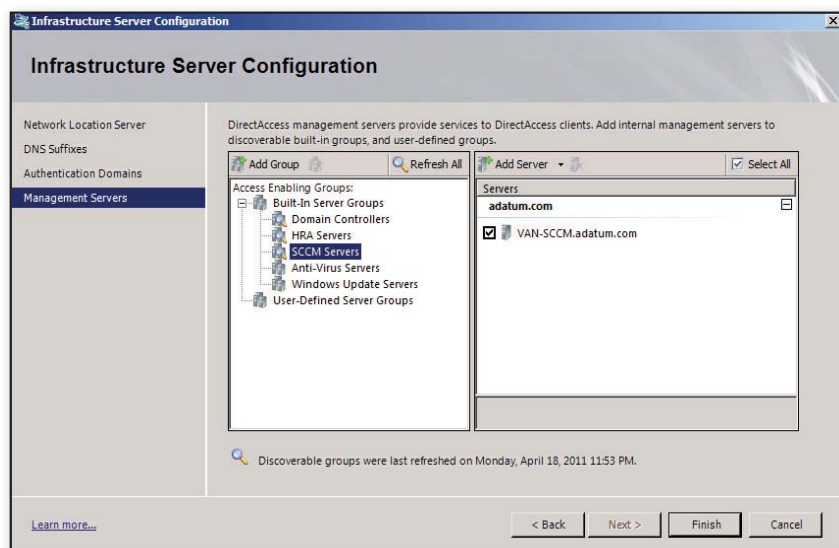


Figure 2: Automatic discovery of SCCM servers

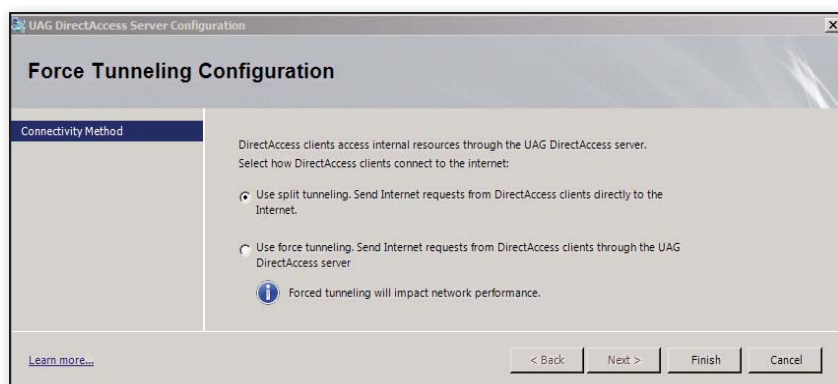


Figure 3: Enabling force tunneling behavior

worried that clients connecting from open wireless networks (such as those found in hotels, coffee shops, and airport lounges) could be targets for attack. In such networks, an attacker could steal authentication cookies from HTTP connections and impersonate the user, or manipulate name resolution to perform man-in-the-middle attacks. Not using split tunneling ensures that all communication from the client is sent in a secure channel to the internal network, blocking those attacks and making sure the client is adhering to the organization's policies when browsing the Internet.

Forefront UAG SP1 lets you change the DirectAccess behavior from split tunneling to force tunneling, as Figure 3 shows. When force tunneling mode is enabled, all client communication is sent through the DirectAccess server, with the exception of local subnet traffic. All names are resolved by the internal DNS servers regardless of the namespace.

Force tunneling comes with a price. When force tunneling is enabled, all traffic from the client is transported to the DirectAccess server over HTTPS using the IP-HTTPS interface, introducing another layer of encryption in addition to IPsec. The double encryption increases CPU consumption on the DirectAccess server, which also must cope with the additional traffic from the client to the Internet. A Forefront UAG DirectAccess server supports significantly fewer concurrent users in force tunneling mode than in split tunneling mode.

The biggest impact, though, might be in terms of application compatibility. With force tunneling, all traffic from the DirectAccess client can use only the IPv6 protocol, because the traffic must go through the DirectAccess tunnels that are

IPv6 only. (IPv6 isn't required on the server side, because Forefront UAG can translate the client traffic to IPv4 using NAT64.) Client applications that don't support IPv6, such as Microsoft Communicator, won't be able to communicate even to IPv4 hosts on the Internet and can't be used on DirectAccess clients with force tunneling.

Although Microsoft supports the use of DirectAccess with force tunneling, this mode should be used only when absolutely necessary. In addition, organizations should carefully evaluate and test this option before enabling it in a production environment.

One-Time Password Authentication

For many organizations, two-factor authentication is a must-have for any remote access service. In its first release, DirectAccess offered two-factor user authentication using smart cards; Forefront UAG SP1 introduces support for authentication using OTP tokens, such as RSA SecurID. OTP authentication is used to authenticate the IPsec intranet tunnel; only users in possession of the token can connect to servers on the internal network.

One of the challenges Microsoft faced to incorporate support for OTPs in DirectAccess was the fact that Windows's IPsec implementation can't use OTP credentials. Forefront UAG SP1 goes around this limitation by using OTP authentication to issue users a short-lived certificate, which is then used to authenticate the IPsec intranet tunnel. Figure 4 shows how the authentication process works.

1. When an application tries to connect to an internal server, the DCA tool prompts the user for his or her OTP credentials.
2. The user enters the OTP credentials, and the DCA tool sends the credentials over HTTP to a special OTP web portal trunk created on the Forefront UAG SP1 server.
3. The Forefront UAG SP1 server contacts the OTP server to authenticate the credentials. Forefront UAG ships with the RSA SecurID agent, but any Remote Authentication Dial-In User Service (RADIUS)-based solution that's compliant with the OATH standard can be used.
4. If the authentication is successful, the Forefront UAG SP1 server requests a short-lived user certificate from a certification authority (CA). Microsoft recommends that a dedicated CA is used to issue these certificates, which by default are valid for only 8 hours or while the user is logged on to the machine, whichever comes first.
5. The Forefront UAG SP1 server replies back to the DCA tool with the short-lived user certificate, which is then used to authenticate the IPsec intranet tunnel and enable access to the internal network. When the certificate expires, the

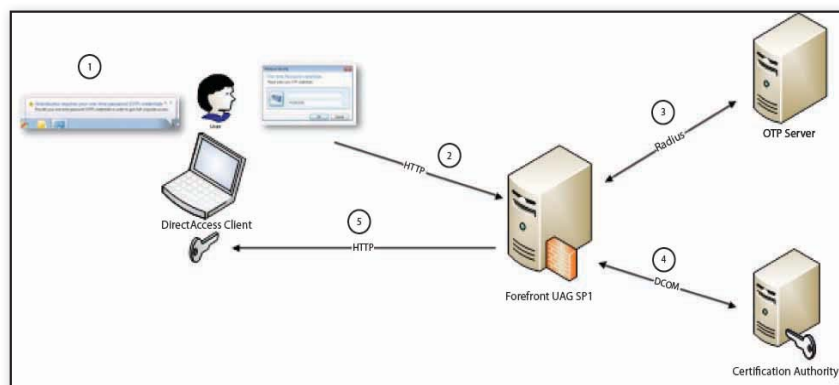


Figure 4: OTP authentication process

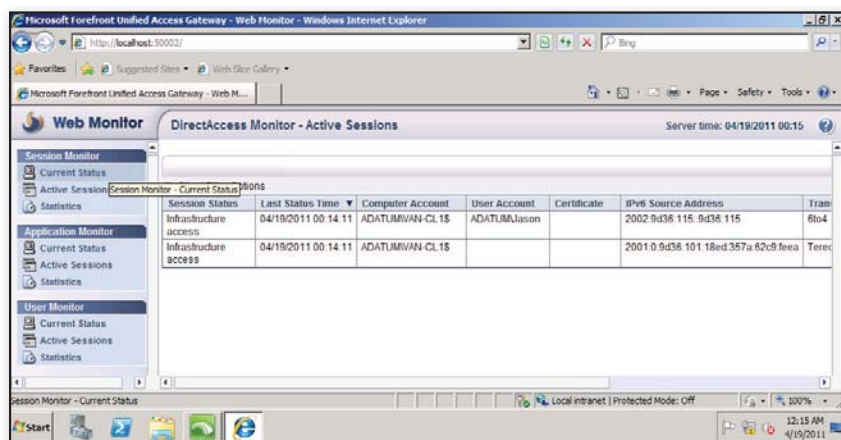


Figure 5: DirectAccess monitoring with the Forefront UAG Web Monitor tool

process starts again with the user being prompted for a new OTP.

A key piece of the underlying infrastructure is the CA that issues the short-lived certificates. This CA needs to run on a Server 2008 R2 server, and it can't be the same CA that issues the machine IPsec certificates, nor can it be one of that CA's parents. To simplify deployment, Forefront UAG SP1 includes a PowerShell script that configures the appropriate certificate templates and permissions on the CA server.

The OTP authentication support lets organizations preserve the investments they've made in deploying OTP tokens for VPN or remote web access. In addition, OTP authentication eliminates one of the most common deterrents to DirectAccess deployment.

Monitoring and Logging

Another area of improvement is monitoring. Forefront UAG SP1 introduces integrated monitoring of DirectAccess connections in

the Forefront UAG Web Monitor tool. The DirectAccess monitor provides a list of currently logged on users, including machine and user account, IPv6 source address, level of access (infrastructure or intranet), and health status if NAP is being used.

This information, which Figure 5 shows, is persisted in the local SQL Server database. You can use the Forefront Threat Management Gateway (TMG) management tool, which is also included in the Forefront UAG SP1 installation, to view the historical data. You can also configure logging to a remote SQL Server machine, which is great for consolidating logs from servers in an array.

Speaking of arrays, the Web Monitor tool now includes a consolidated status view of all the DirectAccess servers in an array, indicating the health condition for each array member, as Figure 6 shows. The Web Monitor tool can be used remotely from any browser, providing operators an easy way to quickly check the status of the DirectAccess infrastructure.

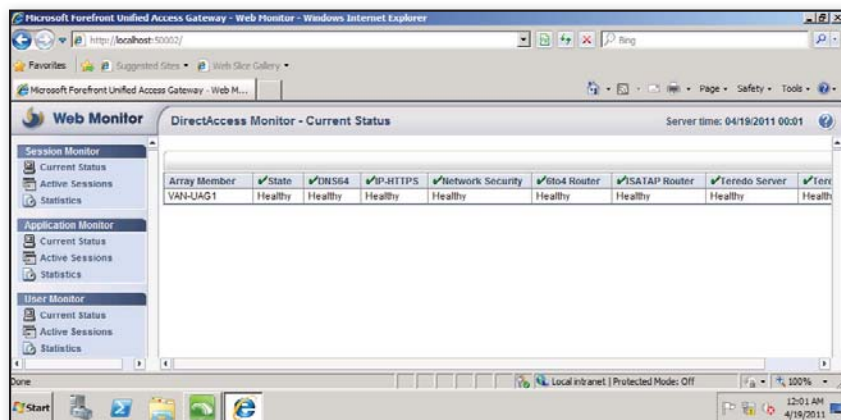


Figure 6: Health monitoring of Forefront UAG array members

Easier Deployment

Forefront UAG SP1 incorporates several improvements to ease DirectAccess deployment. The UAG DirectAccess Configuration Wizard can now configure DirectAccess settings across multiple domains, as well as use existing GPOs for client, gateway, and application server configuration instead of creating new ones. The flexibility also exists to link these GPOs to organizational units (OUs) instead of using groups and to customize the names of the GPOs directly from the wizard.

NAP configuration is also integrated into the UAG DirectAccess Configuration Wizard. If NAP is selected, Forefront UAG SP1 sets up Health Registration Authority (HRA) and Network Policy Server (NPS) on the UAG server and configures the network policies for reporting and enforcing system health requirements on the DirectAccess clients. The NAP components report into the Forefront UAG monitoring and logging infrastructure, so administrators can see the latest information in the Web Monitor tool and query the SQL Server database for historical data about client health status.

On the client side, the DCA tool configuration is now part of the UAG DirectAccess Configuration Wizard, and its settings are incorporated into the client configuration GPO. Deploying the tool still isn't part of the wizard, but because the tool installation package consists of a single Windows Installer (MSI) file, organizations could even use the same GPO to install it.

An All-Around Better Solution

Overall, Forefront UAG SP1 is a huge step forward in making DirectAccess more secure, simpler to deploy, and easier to operate. With the increasing mobility of the workforce and the trend toward deperimeterization reaching many enterprises, no Windows 7 deployment is complete without a remote access and management technology—and DirectAccess is now an even stronger contender for this role.

InstantDoc ID 129973



Fernando Cima

(fcima@microsoft.com) is a security architect at Microsoft Consulting Services, working for the Middle East and Africa team, based in Dubai (UAE). He designs and deploys secure network access solutions for Microsoft enterprise customers.

Hyper-V Disk Configuration Options

Creating virtual machines (VMs) in Microsoft Hyper-V is a snap: You simply right-click New and select Virtual Machine. In a few short moments, you can be working with a brand-new VM. After you install an OS and some applications, you have a new production server ready for use.

However, simply creating VMs inside Hyper-V and immediately going to work isn't the best approach. You need to consider the repercussions of the decisions you make during VM creation, because your actions can introduce problems down the road—particularly performance problems. One of the most important decisions you must make is your choice of Hyper-V disk format.

You're surely familiar with Virtual Hard Disks (VHDs), which is the virtual disk format that Hyper-V uses (as do other hypervisors). But you might not be aware that VHDs are only one of many disk formats Hyper-V can use. Even VHDs themselves have different configurations, each with capacity and performance implications. Understanding the differences between disk formats will help you determine which type of disk to use in your various Hyper-V implementations.

VHDs: Fixed, Dynamic, Differencing

By default, new VMs are created with an attached VHD. These disks represent Microsoft's open format for virtual disks, and they have some very useful benefits. Hyper-V, even in its R2 version, requires boot disks to be IDE. All other disks can be SCSI. But before you consider this a performance bottleneck, you should know that both IDE and SCSI disks in Hyper-V leverage the same VM bus, which results in functionally similar performance between both disk types.

Nevertheless, SCSI VHDs include some additional features that make them a better choice for all but your OS drive. SCSI VHDs can be hot-added in Hyper-V R2. In addition, SCSI VHDs have higher limits on size and quantity, with SCSI disks supporting sizes up to 2TB. You can also add many more SCSI disks to a VM, circumventing IDE's four-disk limitation. For these reasons alone, it's considered a best practice to use Hyper-V's SCSI disks for everything except storing your core OS.

Another important consideration with Hyper-V disks is managing storage capacity. Hyper-V has three options for creating new VHDs: fixed size, dynamically expanding, and differencing. As you can probably guess, fixed-size VHDs provision the entire disk size as the disk is created. Dynamically expanding disks consume only as much space as is actually used by data on the disk.

In the first version of Hyper-V, the performance difference between fixed and dynamic disks was fairly significant—enough so that Microsoft recommended using fixed disks for

Configure your
virtual disks
for optimal
performance
and useability

by Greg Shields

■ HYPER-V DISK OPTIONS

all production workloads. Hyper-V R2 reduces this difference somewhat, with Microsoft now reporting that dynamic disks see between 85 percent and 94 percent of fixed disk performance. (This 9-percent span in performance has much to do with the type of workload for which the disks are being used.)

In the white paper “Virtual Hard Disk Performance: Windows Server 2008/Windows Server 2008 R2/Windows 7” (download.microsoft.com/download/0/7/7/0778C0BB-5281-4390-92CD-EC138A18F2F9/WS08_R2_VHD_Performance_WhitePaper.docx), Microsoft reports on the performance of applications that the company tested across a series of workloads. According to Microsoft’s findings, fixed VHDs in all workloads performed better than their dynamic counterparts; however, the difference in many cases was exceptionally slight.

Although performance should be a key factor in your fixed versus dynamic decision, you should also remember that fixed disks increase your storage costs. When you use fixed disks, you consume storage for what amounts to empty space. If your organization has limited storage space or simply doesn’t want to spend money on wasted storage, you should consider trading a slight performance degradation for higher storage utilization.

Differencing VHDs let you link multiple VHDs to one another. Child VHDs begin their lives with the same set of data as the parent disk; they only increase in size as their data changes in comparison with the parent disk. Although Microsoft’s performance tests found that differencing disks experience about the same level of performance as dynamic disks, you need to take special care with these kinds of differencing disks because of their dependencies on one another. Differencing disks are linked to each other, and in fact multiple differencing disks can be linked together to create a chain of disks. As a result, although the storage consumption of these disks can be less than that of other disk types, this benefit must be considered alongside the risk of inadvertently breaking the disk linkage.

Microsoft doesn’t officially suggest not using differencing disks; however, these disks are most often relegated to nonproduction scenarios. One production implementation in which they’re often used is in Virtual Desktop Infrastructure (VDI) architectures, where child VHDs are provisioned from a master reference image (sometimes called a *golden image*). Because virtualized desktops tend to remain very similar to their parents and can be easily discarded when users are finished with them, this pairing can be a good idea if you’re considering VDI desktop deployment.

Pass-Through Disks

Yet another type of disk, called a pass-through disk, isn’t a VHD at all. These disks are created by attaching a disk volume to a Hyper-V host, typically through either an iSCSI or Fibre Channel connection. After the disk volume is attached to the Hyper-V host, the disk is then *passed through* to an awaiting VM—hence the name.

Unlike VHDs, pass-through disks don’t encapsulate data into a virtual disk format. Their raw format lets data remain in the standard NTFS format on the SAN. Keeping data in its native format can improve the backup and restore process, as well as eliminate the 2TB limitation of VHDs.

Further results from Microsoft’s white paper “Virtual Hard Disk Performance: Windows Server 2008/Windows Server 2008 R2/Windows 7” (download.microsoft.com/download/0/7/7/0778C0BB-5281-4390-92CD-EC138A18F2F9/WS08_R2_VHD_Performance_WhitePaper.docx) suggest that pass-through disks experience better performance than fixed VHDs across every scenario, although the performance difference is slight. This might be because a lower level of CPU utilization is required for addressing data on a pass-through disk. Another reason might be improved sector alignment on the SAN (i.e., the sectors that comprise the disk volume are correctly aligned with the sectors that are recognized by the SAN hardware). Misalignment between the volume and the SAN is often a cause of poor disk performance.

Although pass-through disks are first connected to the Hyper-V host, they do support Live Migration. In fact, pass-through disks have been reported to see better Live Migration performance than VHDs because of the fact that the VM doesn’t need to mount the disk’s file system during a Hyper-V Live Migration.

Pass-through disks have their own disadvantages—the greatest of which is the fact that they don’t enjoy the typical benefits gained by disk virtualization. Another drawback is that pass-through disks’ initial connection to the Hyper-V host can require additional management and due diligence, particularly in the case of VMs that participate in a host cluster. Proper masking and zoning to Hyper-V cluster hosts is required but can cause administrative headaches because each pass-through disk can be used by only one VM. Finally, you can’t back up pass-through disks through the Hyper-V VSS writer and thus any host-based backup solution. Therefore, your backup and restore tactics will require either backing up the disk’s LUN from the SAN or via an agent installed on the VM.

Many Options, No Correct Answers

Hyper-V offers a wide range of options for configuring VM disks: IDE or SCSI, fixed or dynamic, VHD or pass-through. However, there’s no absolutely correct answer regarding which options you should choose. Some disk configurations work well in certain circumstances but not in others. Other configurations fix some limitations but add other caveats. The moral of this story is to carefully plan your disk configuration before you ever click New, Virtual Machine. A little extra thought in the beginning can save you a substantial headache down the road. (For information about creating virtual disks on VMware ESX VMs, see “VMware ESX Disk Configuration Options,” InstantDoc ID 129975.)

InstantDoc ID 129974



Greg Shields

is a partner and principal technologist with Concentrated Technology, an IT analysis and strategic consulting firm. Contact him at www.ConcentratedTech.com.

VMware ESX

Disk Configuration Options

VMware ESX offers several options for creating virtual disks (i.e., VMDK files) for virtual machines (VMs). This article covers options for thin and thick VM disk provisioning, along with general recommendations for storing VMDK files on ESX DAS and SANs. It's especially important to consider block size when formatting an ESX storage group, or you might have to back up any existing VMs and reformat the storage group. These disk configuration parameters have a significant effect on functionality, performance, and manageability.

Creating a Disk

When you add a disk to a VM in VMware ESX, you're prompted with options to create a new virtual disk, use an existing virtual disk, or create a raw device mapping. The first two options are self-explanatory. When a raw device mapping is stored on a SAN, the files aren't encapsulated inside a VMDK file. If you browse the files on the SAN LUN, the individual files will appear, not just a single VMDK file that encapsulates all the files inside the VM's disk.

If you have a SAN, you can create a raw device mapping that maps storage to a LUN on the SAN. Raw device mapping can give you better throughput for sequential disk I/O and similar performance for random disk I/O compared with non-raw device mapping disks. But the main reason to use raw device mapping is if you need to expose the physical device properties for SAN management software.

Raw device mapping can be configured in virtual or physical mode. Virtual mode presents the raw device mapping just like any other VMDK file, with all the same functionality of a regular VMDK file, such as snapshots and cloning. Physical mode exposes all the physical hardware, with the exception of the REPORT LUNS command, which is virtualized so that ESX can track which VM is using the LUN.

Some SAN vendors' VSS writers that are used for SAN snapshots, backup, or replication require the use of a raw device mapping in physical mode. However, raw device mappings in physical mode prevent you from using VMware snapshots, cloning, and VMotion on the VM. Physical mode is required by some SAN vendors to ensure that the VMs are properly quiesced before a SAN snapshot is taken.

Quiescing is important for VMs running any type of logged data changes, such as Microsoft Exchange Server and Microsoft SQL Server. Quiescing temporarily stops transaction flow on the VM so that when a SAN snapshot is taken, only fully complete transactions reside in the database. If a VM isn't properly quiesced, you run the risk of snapping a VM with a database in a "dirty" (partial transactions) state.

Raw device mapping disks can be used instead of a large VMDK file (over 1TB) if you don't feel comfortable storing that much data in a single VMDK file. Check with your SAN vendor for more information about raw device mapping.

Disk Provisioning

You can choose either thick or thin disk provisioning when you create a VM disk. If you select thick provisioning, ESX will allocate the entire size of the disk on the storage group when it's created. If you

Increase
functionality,
performance,
and
manageability

by Alan Sugano

Table 1: SCSI Controller Type Based on Windows OS

Windows OS	SCSI Controller
Windows 2000 Server and earlier	BusLogic Parallel
Windows Server 2003	LSI Logic Parallel
Windows Server 2008 R2 and Windows Server 2008	LSI Logic SAS or LSI Logic Parallel

Table 2: Relationship Between Block Size and Storage Group File Size

Block Size	Maximum File Size
1MB	256GB less 512 bytes
2MB	512GB less 512 bytes
4MB	1TB less 512 bytes
8MB	2TB less 512 bytes

thin-provision a drive, only the space that's used in the VM disk is allocated. Thin provisioning saves storage space, but you'll take a performance hit and increase the probability of running out of space on the ESX storage group.

The performance hit of thick versus thin provisioning is based on many factors, including disk speed, array configuration, and degree of disk fragmentation. As a general rule, thick provisioning gives the best performance and reduces the chance of running out of disk space. Although it requires more disk space, it's a more conservative approach.

If you plan to thin-provision your VM disks, I suggest using it only for VM base images rather than data drives for VMs. If you create several VMs with 1TB thin-provisioned data drives, and users start saving data on these drives, you might very quickly run out of disk space on the ESX storage group.

Disk and Controller Types

When you create a VM, you have the option of creating either IDE or SCSI disks. You should use SCSI disks whenever possible, because they provide better performance than IDE disks. You might have to use IDE disks if the VM's application doesn't support SCSI disks.

You must select the SCSI controller type when creating disks. The Windows OS determines the type of SCSI controller to use, based on compatibility and performance. Table 1 lists controller types by Windows OS.

In addition to the SCSI controllers listed in Table 1, you can also use the VMware

Paravirtual driver. However, you should use the Paravirtual driver only if the drives are stored on a SAN and not using DAS; the VM will require more than 2,000 I/O operations per second of disk throughput; the VM will run Windows Server 2008 R2, Windows Server 2008, Windows Server 2003, or Red Hat Enterprise Linux (RHEL) 5; the drive isn't a boot disk; the VM isn't fault-tolerant; and the VM won't be used as part of a Microsoft cluster. As a general rule, using the VMware Paravirtual driver gives you about 10-percent better disk throughput and 15-percent lower CPU utilization than using the LSI Logic SCSI controller when the VMDK file is stored on a SAN.

Independent Disks: Persistent vs. Nonpersistent

After selecting the disk type (IDE or SCSI) and the controller type, you have the option of creating an independent disk. You might use an independent disk if you don't want the disk to be affected by snapshots.

In general, you should leave the Independent check box blank, unless you need this feature. If you decide to create an independent disk, you have two additional options: persistent and nonpersistent. With persistent disks, any changes are immediately and permanently written to disk, even when a snapshot is taken of the VM. With nonpersistent disks, any changes to the disk will be discarded when the VM is rebooted or reverted back to a snapshot. The only time you might want to use this setting is in a lab environment if you want the VM to go back to its original state when it's rebooted. Because this is such a dangerous hacking tool, I suggest reviewing the drive configuration of all VMs on a regular basis to verify that they aren't configured with any nonpersistent disks.

Storage Group Block Size

One item that haunts administrators who are new to ESX is the block size when a storage group is formatted. The block size

determines the largest VMDK file that can be created on the storage group. The block size is independent of the total size of the storage group. Table 2 shows the relationship between block size and storage group file size.

The default block size is 1MB, so you can only create a VMDK file that's 256GB less 512 bytes. If you need to create a VMDK file that's larger than 256GB, you must back up your data, format the storage group with a larger block size, and restore the VMDK files—which isn't a lot of fun in a production environment.

If you want to retain a VM's snapshot functionality, make sure to create a VMDK file that's 2GB smaller than the maximum allowed file on the storage group. For example, if you have storage that's formatted with a 1MB block size, you shouldn't create a file larger than 254GB. If you create a VMDK file that's 256GB on the storage group, you'll receive an error that the VMDK file exceeds the maximum file size on the storage group when you attempt to snapshot the VM. When a snapshot is created, the original VMDK file creates a 2GB stub file. So, if you try to snapshot a VM that has a 256GB VMDK file, ESX tries to create a VMDK file that's 258GB and the snapshot fails.

Choose Your Options Carefully

You have many options for creating VM disks on VMware ESX. Some of these options are available only if your VM disk is stored on a SAN. Probably the biggest pitfall is the storage group block size, because it's difficult to change. Choose your disk configuration carefully to ensure the best combination of management, cost, performance, and functionality for your VMs. (For information about configuring VM disks on Microsoft Hyper-V, see "Hyper-V Disk Formats," InstantDoc ID 129974.)

InstantDoc ID 129975



Alan Sugano

(asugano@adscon.com) is the president of ADS Consulting Group, which specializes in virtualization, networking, custom programming, Microsoft .NET web development, and SQL Server development. He's the author of *The Real-World Network Troubleshooting Manual* (Charles River Media).

Integrating Mobile Platforms with Exchange Server 2010

Choosing a mobile platform for business purposes is more difficult today than ever before. Only 3 years ago, things were much simpler—enterprises used Windows Mobile or BlackBerry. Today, many platforms are competing in this market segment, and the decision of which to use is much more difficult to make. As B. K. Winstead explains in his article “Smartphones in the Enterprise: Opening Pandora’s Box” (July 2010, InstantDoc ID 125318), each platform has its strengths and weaknesses, and vendors are mostly trying to balance between consumers and business users by providing the same type of devices for both. In “Smartphones in the Enterprise,” Winstead provides a big-picture view of the smartphone market; in this article, I narrow the story to one specific service: Microsoft Exchange Server integration.

Because so many enterprises use Exchange as a collaboration platform, the level of integration between a mobile platform and Exchange can be an important factor in adopting it. In addition, because Microsoft provides its ActiveSync protocol to any vendor that wants to implement it, this protocol has become standard. Almost every mobile platform now supports ActiveSync. However, many factors affect the decision of which mobile platform will best integrate with Exchange in your environment.

Integration Basics

In general, what we expect from a mobile platform is the ability to synchronize our email messages, contacts, and calendar from our Exchange mailbox to a mobile device, as well as Direct Push support. Some more demanding users will probably also expect to have tasks and maybe even notes synchronized on their mobile device. And although mobile devices are mostly focused on consuming rather than producing content, you can typically expect the ability to create or update a meeting request from your mobile device, edit a contact in your Exchange address book, create a new task or note, and perform email management tasks such as accessing other folders in the mailbox, managing out-of-office features, and more. Another nice feature to have would be Microsoft Information Rights Management (IRM) support so that you could open encrypted email messages and send digitally signed emails. Some platforms support synchronization of text messages (SMS) to the Exchange mailbox, but most platforms use their own solution to accomplish this task.

For systems administrators, the most important aspects of integrating a mobile platform with Exchange are device control, provisioning, and management. Various solutions for mobile platform management exist (e.g., Microsoft System Center Mobile Device Manager), but for this article, I focus on management policies that are available with Exchange. Exchange Server 2010 and Exchange Server 2007 offer policies through the ActiveSync protocol that provide an acceptable level of device control.

Exchange ActiveSync (EAS) lets you force password requirements to a mobile device, configure the amount of data that will sync from your Inbox and calendar, and allow or prohibit synchronization while roaming. In addition, you can control some basic application usage on the device (e.g., browser

Finding the
perfect solution
amid imperfect
options

by Damir Dizdarevic

and email clients), as well as some hardware capabilities such as Bluetooth, wireless, camera, and storage card access. You can also configure allowed or blocked applications that can (or can't) run on the device. In general, these settings provide the most important features for managing mobile devices. All these settings are mandatory: if they're applied, users can't change them from the client side.

These policies are created on the Client Access server role's organization level in Exchange 2010 and Exchange 2007. They're applied on a per-user basis, which means you can create different policies for different users. However, the policies can be applied only up to the level that the mobile device supports. Policy settings that the mobile platform doesn't support on the client side are simply ignored.

Before you decide on a mobile platform to implement in an existing Exchange Server environment, it's helpful to know what you can expect from each platform regarding Exchange integration. In the following sections, I discuss Exchange integration with Windows Mobile 6.5, Windows Phone 7, Apple iOS 4.3, and Google's Android 2.2.

Platforms of Choice

Although numerous mobile platforms exist, I decided to focus on just four: Windows Mobile 6.5, Windows Phone 7, iOS 4.3, and Android 2.2. Before I get too far into the discussion, let me explain why I chose these platforms: I wanted to test Exchange integration with mobile platforms that have the ActiveSync client natively implemented in the OS rather than provided as a third-party application.

You might wonder why I included Windows Mobile 6.5 when everyone is neglecting this platform today. The answer is simple—if we're just looking at Exchange integration, Windows Mobile 6.5 still has much to offer. Windows Mobile 6.5 actually supports all the features and integration capabilities that I discussed in the previous section, whereas no other platform fully supports all these elements. The disadvantage of this platform is that Microsoft has stopped developing it, so we probably won't see any new applications for it. Although Microsoft promised that the company will continue to provide support

for Windows Mobile 6.5, no one knows what kind of support, or to what extent. If you already have Windows Mobile 6.5 deployed in your enterprise, you can keep using it for the foreseeable future—but if you're thinking about deploying mobile devices from scratch, you should probably avoid this platform.

I also didn't include BlackBerry, which is a very popular mobile device, especially for business-oriented users. The main reason for this omission is because the BlackBerry platform doesn't provide native Exchange support. To sync your BlackBerry with Exchange, you must buy BlackBerry Enterprise Server (BES) for Microsoft Exchange. Although some workarounds exist to enable ActiveSync on BlackBerry without BES—that is, through third-party client applications—I decided to drop the platform from my discussion because it doesn't provide a unified experience.

Windows Mobile 6.5.x Professional.

When it comes to ActiveSync implementation, Windows Mobile 6.5.x Pro is the most complete platform you can find. This platform provides full integration capabilities. You can apply all available Exchange policies (from Exchange 2010 to Exchange Server 2003) to Windows Mobile 6.5 Pro. In addition to synchronizing your calendar, email, and contacts, Windows Mobile 6.5 lets you sync tasks and notes (via Microsoft Windows Mobile Device Center, which also gives you the ability to sync files, photos, and videos between your device and computer). If you're using Exchange 2010, you can also sync text messages to your Exchange Inbox. In fact, Outlook and Outlook Web App (OWA) can use ActiveSync to send text messages (SMS) to your mobile device, which then uses the mobile network to forward the messages to recipients. In the other direction, each message that comes to your mobile device is forwarded to your mailbox on Exchange.

Windows Mobile 6.5's email management is quite advanced. You can easily configure certificate usage, and you can specify whether you will sign or encrypt email messages that you send from your device. You can also open digitally signed and encrypted email messages, with the option to check certificate validity. The platform also lets you use device certificates for authentication.

Windows Mobile 6.5 supports mobile Outlook's conversation view in Exchange 2010. In addition, the platform supports over-the-air updating of Outlook Mobile client software.

The biggest disadvantage of Windows Mobile 6.5 is more than obvious: The platform is a dead end. Another disadvantage is the fact that the platform isn't very finger-friendly and instead requires a stylus, although that problem can be mostly solved by implementing a vendor-produced interface such as HTC Sense. Very demanding users will also complain about the platform's inability to support multiple Exchange accounts.

From an administrator perspective, Windows Mobile 6.5 is a dream platform. In addition to providing full support for Exchange policies, the platform can be managed and provisioned by using System Center Mobile Device Manager 2008, it can be authenticated by using client certificates, and it can even be enrolled in a domain.

Windows Phone 7. Interestingly, the ActiveSync capability isn't one of the features that's highlighted in Windows Phone 7 marketing. You can find a lot of information about every single feature of Windows Phone 7—except Exchange integration and ActiveSync implementation. After testing the Windows Phone 7 platform, I understand why. The truth is that Windows Phone 7 lacks many of the ActiveSync features that Windows Mobile 6.5 includes.

Windows Phone 7 has a lot of great features. For example, you can configure multiple Exchange accounts (which are now called Outlook accounts, to align with Office Mobile terminology). The email client is fast, user-friendly, and extremely easy to use. The calendar is likewise easy to use, with the capability to check users' availability and to show events from multiple calendars. An important enhancement related to contacts is that they fully integrate with other address books, such as Facebook and Windows Live address books. Windows Phone 7 can also import pictures from Active Directory (AD), which can be convenient.

Missing features in Windows Phone 7 include the ability to sync tasks, notes, or text messages from Exchange. Although you can configure multiple Outlook accounts, the platform lacks a unified email

Inbox, and conversation view isn't supported. Windows Phone 7 doesn't provide IRM support for email messages. You can still conveniently flag email messages, but this is about the most advanced thing you can do with your email. Finally, you can't search messages that aren't cached on the device but that are located on Exchange.

I tried applying Exchange policies to Windows Phone 7 but found that only the most basic policies can be applied (e.g., enforcing the device's password, desktop synchronization, remote wipe-related options). If your Exchange server has other policies configured—for example, device encryption—Windows Phone 7 generates an error message during synchronization (error code 86000C2B). In addition, you can't use System Center Mobile Device Manager to manage Windows Phone 7. If you want to support Windows Phone 7 devices but also enforce policies on Windows Mobile 6.5 devices that the Windows Phone 7 platform doesn't support, you must select the option *Allow non-provisionable devices* in Exchange Server's EAS policy.

Although no critical Exchange features are missing, Windows Phone 7 lacks quite a few advanced features. Business users will probably miss synchronization of tasks and notes, as well as the unified Inbox feature and conversation view. We can only hope that the growing mobile market will soon provide some relevant third-party apps.

From an administrator's perspective, Windows Phone 7 is a very closed platform. Currently, no tools are available for application management or device provisioning. The question remains, Does a platform exist that not only has a future but also serves users who expect all of Windows Mobile 6.5's Exchange-related features?

iOS 4.3. Since the first iPhone release 4 years ago, which had no Exchange support at all, Apple has made great progress in this field. Apple's current platform, iOS 4.3, is available on 3GS and iPhone 4 devices and includes a large number of ActiveSync features. When iOS 4 was released, it was the only platform available that supported more than one Exchange account (until Windows Phone 7's release). iOS 4.3 natively supports the conversation view and provides a unified Inbox, which is extremely useful for users who have more than one email account on their phone.

iOS 4.3 has another extremely useful feature: It can synchronize the Suggested Contacts folder. This folder contains all the email addresses that you typed or replied to in desktop Outlook but didn't save to your address book. Each time you start typing an email address in Outlook or OWA, you're presented with a list of addresses that you've used. On previous versions of Exchange (and Outlook), these addresses are located on the local machine, in a .nk2 file. On Exchange 2010, this data is migrated to the user mailbox in the Suggested Contacts folder. iOS 4.3 can sync that folder to your phone—and in fact is currently the only platform that can. Also, iOS 4.3 lets you perform a message search on Exchange Server, which means that you can search your whole mailbox from an iOS device.

iOS 4.3 lets you easily search the Microsoft Exchange Global Address Book. In addition, you can use the calendar application to create invitations, as well as accept or decline them (or say "maybe"). Advanced features such as contact availability aren't included.

On the downside, iOS 4.3 doesn't sync tasks natively (although the App Store offers several apps that provide this capability). You can sync notes, but only from Outlook, using iTunes installed on Windows. IRM isn't supported for email messages, and you can't flag email messages or access out-of-office features from your phone.

Applying Exchange policies in iOS 4.3 works better than I expected. iOS 4.3 fully supports password policies, as well as basic policies for content synchronization and synchronization during roaming. You can also use Exchange policies to disable the camera, Wi-Fi, and the Safari browser on the iPhone. Of course, you can't control applications installed from the App Store, nor can you provision devices with iOS (at least not with Microsoft tools). iOS 4.3 also supports certificate authentication.

Android 2.2. Android has become an attractive choice for all kinds of customers, with the most extensive growth in the past year. However, Exchange support has never been extensive in the platform. The current version, Android 2.2 (code-named Froyo), has several Exchange enhancements compared with the previous version—but still not enough to compete with iOS or

Windows Mobile 6.5. The upcoming version, Android 2.3, doesn't seem to provide any new Exchange features either.

Android 2.2 supports the conversation view, as well as email flagging. Navigating the Exchange Global Address Book is relatively easy. The email client is fairly simple and easy to use, but it's not very Exchange friendly. You can manage out-of-office features from Android—which is surprising, but it's a useful capability. Android's calendar is good, but sending a meeting invitation occurs from the email application, not from the calendar during item creation—which is an odd solution.

Perhaps the most irritating Exchange-related oversight on Android is the lack of support for reply and forward tags on email items. If you reply to a message (or forward it) from your mobile device, the message is marked as replied on the mobile device but not in Outlook or OWA—and vice-versa.

Another drawback is the inability to push items in any other folder than the Inbox. You can configure Direct Push, but it works only for the Inbox. If you want to check whether a message has arrived in another folder, you must open the folder and manually initiate synchronization. In addition, you can't search messages that are on Exchange but not cached on the mobile device.

Android 2.2 doesn't support multiple Exchange accounts. Tasks and notes aren't synchronized to mobile devices. Finally, the platform doesn't support IRM.

When it comes to Exchange policies, Android has very little to offer. You can force password policies and perform a remote wipe—but that's about it. Google has a lot of work to do to enhance Android's Exchange capabilities, but it remains to be seen whether the company is willing to do it. A major disadvantage is the inconsistency between mobile device vendors. Some devices have more problems with using the built-in client for Exchange synchronization than others. A possible solution is to use third-party apps for EAS.

Configuring Exchange Synchronization

To truly evaluate a platform's usability, you need to actually use it. Thus, I tested each of the mobile platforms on an appropriate mobile device: iOS 4.3 on an iPhone 4, Windows Phone 7 on an LG Optimus 7,

Windows Mobile 6.5 on an HTC HD2, and Android 2.2 on an HTC Desire.

iOS 4.3. Setting up an Exchange account on iOS 4.3 is a pretty simple task. Select Settings, Mail, Contacts, Calendars, Add Account. You'll be presented with several account options to configure, including Microsoft Exchange, MobileMe, Google Mail, Yahoo, and AOL. Select Microsoft Exchange, then enter the required data to set up your mailbox (i.e., email address, username, and password). iOS 4.3 uses Autodiscover and will try to find your Exchange server automatically. After your credentials are verified, you might need to enter a server name (which should be your Client Access server public name). On the next screen, you can select which items to synchronize (mail, contacts, calendar). By default, iOS synchronizes the past 3 days of email, from the Inbox folder only. However, you can easily add more folders and specify a wider time range, simply by revising the account properties after configuration. You can run into problems with Exchange account setup if your Client Access server is equipped with a nontrusted certificate. In that case, iOS will ask whether or not you trust that server. You can use the same procedure to add more Exchange accounts (or other types of accounts), which will be synchronized into one unified Inbox.

Windows Phone 7. Windows Phone 7 is definitely the easiest platform on which to set up an Exchange account—if your Exchange server is configured correctly and has a widely trusted certificate installed. If, however, you use a certificate issued by your own internal Certification Authority (CA), you must add the root CA certificate to the list of the trusted CAs on your device. One method of accomplishing this task is to send the CA certificate to a public email address (such as Hotmail or Gmail) and synchronize this mailbox with your device (which you can accomplish without an SSL certificate, then retrieve the certificate from email).

Another option is to connect Windows Phone 7 on your corporate network's Wi-Fi, connect to your CA's web enrollment page, and download the certificate from there. Then, go to Settings, select *email & accounts*, and choose Outlook (the Exchange mailbox is called Outlook in Windows Phone 7). You'll be prompted for your email address and password; all other data

is retrieved through Autodiscover. After the account is configured, you can specify how much data will sync to your device and you'll be able to use Direct Push.

Windows Mobile 6.5. To completely set up ActiveSync on Windows Mobile 6.5, you have to spend more time than on iOS 4.3 or Windows Phone 7. This isn't because the setup is more complex, but because more options are available.

To set up an Exchange account, go to Settings and click the ActiveSync icon. After the application opens, select Menu, then select the Add Server Source option. Enter your email address on the first screen. You can also select the option to detect Exchange Server settings automatically, which is recommended. Next, provide your username, password, and domain; select the option to save this information for future use. After you complete these steps, the ActiveSync client will use Autodiscover to try to discover your Exchange settings. You can skip this step if it takes too much time, and provide the Exchange server name manually instead. If you choose to do so, or if Exchange wasn't detected automatically, you can also specify whether to use an SSL connection. Finally, you must specify what to sync. In Windows Mobile 6.5.x on Exchange 2010, you have the following options: contacts, calendar, email, tasks, and text messages. Some options, such as email, have additional settings where you can select the amount of data to be synchronized (in days), message format, item size limit, and email encryption. You can also configure certificates for digital signing.

If you decide to synchronize text messages, be aware that this feature doesn't work on all Windows Mobile 6.5 devices. In fact, it works only on devices on which no third-party messaging client is installed. For example, most HTC devices have an HTC Messaging client as part of the HTC Sense interface and can't sync text messages to or from Exchange Server. Only the default Microsoft client for text messages is capable of synchronizing messages over an ActiveSync connection.

Android 2.2. Setting up Exchange on Android is easy. Select Menu, Settings, Accounts & sync. Then, select *Add account* and choose Exchange ActiveSync. Enter your email address and password. After

you enter your credentials, your mobile device will try to verify the certificate on your server. If the certificate isn't trusted (in my environment, the GeoTrust public certificate wasn't trusted by Android), you should select Continue, or select View if you want to see the certificate details. The client will then try to use Autodiscover to configure the Exchange account. If Autodiscover fails, you'll have to enter the Exchange Server name manually. Otherwise, you'll be presented with options for synchronizing content (email, contacts, calendar). When you're done, select Finish Setup. You can also configure options for Direct Push, the amount of content to be synchronized, and the format of content to be synced (email, HTML, or plain text). Android 2.2 also lets you configure synchronization during roaming, as well as conflict resolution (i.e., if an item is modified on both the device and the server).

The Best Really Is Yet To Come

If Exchange integration and ease of management are your primary considerations in choosing a mobile platform, you have a tough decision ahead of you. (Note that I don't discuss Nokia's Symbian platform because it has no unified native application for Exchange Server synchronization, although most versions of Symbian are on pretty much the same integration level as Android.)

It's more than obvious that what the market needs is a real successor to Windows Mobile 6.5—but whether Microsoft will provide that option anytime soon remains to be seen. For a summary of which EAS features are supported by Windows Mobile 6.5, Windows Phone 7, iOS 4.3, and Android 2.2, see Microsoft's Exchange ActiveSync Client Comparison Table at social.technet.microsoft.com/wiki/contents/articles/exchange-active-sync-client-comparison-table.aspx. 

InstantDoc ID 129619



Damir Dizdarevic

(ddamir@logosoft.ba), manager of the Learning Center at Logosoft in Sarajevo, Bosnia, has published more than 380 articles in various IT magazines. He's an MVP for Windows Server Infrastructure Management, and an MCSE, MCTS, MCITP, and MCT.

SharePoint 2010 Goes Social, Part 1

SharePoint Server 2010 introduces many new features to support social networking. In the first part of this three-part article, I look at the major requirements for social networking and introduce the User Profile Service, which provides one of the foundations for such networking. In the second article I'll discuss how to populate the User Profile through synchronization with LDAP-compliant directories, and in the third article I'll describe the major features that are used to better exploit a major information asset of any organization—its people. Note that the social networking features described in these articles are available only with a SharePoint Server 2010 installation and aren't available in a SharePoint Foundation 2010-only deployment.

Using and understanding the User Profile Service

by Kevin Laahs

Social Networking Requirements

Social networking is all about people. It's about finding the right people and the best information sources to use to deliver business goals.

Often, finding the right people is achieved through a journey of discovery (or some might say a journey of frustration!) that leverages the social connections that exist between people and the skills and expertise they possess. A common challenge in large organizations is that the connections between people are often tacit (i.e., not written down, and known only inside the heads of individuals); no definitive source exists for registering the skills that people have or those that they develop as they progress through their careers.

SharePoint Server 2010 was designed with the social side of information sharing in mind. It provides many features that can be used to find the right people to do the right job by treating people as a significant intellectual asset and placing them at the center of any collaboration.

Finding information about people, including who they know and the skills they possess, is usually just a click away. I say "usually" because building such a social network that ultimately delivers value doesn't just happen by merely installing SharePoint. It requires the buy-in of everyone—from executive support, to IT, to end users—such that the full wealth of the organization can be leveraged.

To generate the greatest value, a network's scope must be across an entire organization and be viewed as a social networking hub. Half-hearted deployments typically result in frustrated users who don't see the value in using the system.

SharePoint architects and administrators therefore need to think about how information about people will be captured and how this information will be kept up-to-date so that it's vibrant and accurately reflects the current intellectual wealth of the organization. If information is correctly gathered and managed, then the organization as a whole benefits because SharePoint takes a people-centric approach, offering linkages between other people and resources.

SharePoint helps you understand the social context between you and other people who contribute to your organization's collateral, which can help you build stronger relationships—sometimes with others who you might not have even known existed before you embarked on your information-gathering task.

Importance of the User Profile

Leveraging people as information assets requires a flexible central store that can hold data about the people in an organization. The data held in such a store needs to be gathered from multiple sources,

because it's common for different types of information about people to be held in special-purpose repositories. For example, project information about projects that people worked on might be held in a different database than organizational information, and people skills and interests might exist only inside the heads of individuals.

The User Profile is at the heart of SharePoint Server 2010's social networking features and is where the vast majority of information about people is stored. The User Profile Service application, managed through SharePoint Central Administration, controls many people-centric features, such as maintenance of entries in the User Profile, synchronization of the profile with other repositories, and My Site settings (which I'll discuss in the last article in this series).

Figure 1 shows the management page of the User Profile Service. Note that some options are also displayed to manage organization profiles; however, I don't discuss this feature because it isn't fully implemented in SharePoint 2010.

When a User Profile Service application is initially provisioned, three main SQL Server databases are created to hold people and social information:

1. ProfileDB—Holds user and organization profile information
2. SocialDB—Stores social tags and notes that are created by users against SharePoint collateral; each tag and note is related to an entry in the User Profile so that we know which user created the tag or note

3. SyncDB—Holds configuration and staging information for synchronizing profile data from external sources such as Active Directory (AD)

You can think of the User Profile as a special-purpose SharePoint list that acts as a directory for people. Its contents can be fuelled from multiple sources, such as AD, other LDAP-compliant sources, and Microsoft Business Connectivity Services (BCS), through synchronization.

Developers can also use many techniques to allow profile updates from other applications, and end users can be authorized to update their own directory entries from their My Site. (A common misconception is that the User Profile is required or involved when authorizing access to a SharePoint site. However, no requirement exists to implement the profile in authorizing access to SharePoint content.)

The User Profile is defined in terms of user properties. You can modify the default set of properties to add other pertinent properties that will help people become better connected. Typically, you'd add properties to hold data that you could either populate and maintain automatically or that the end users themselves could manage. For the latter to be successful, users must know the intended purpose of the property so they can provide pertinent data. What this all boils down to is that there's no point in adding properties to a profile unless you strongly believe they will be useable, maintainable, useful, and will add value. To maximize SharePoint's social

networking capabilities, you should ensure that the data held inside the User Profile is rich, relevant, up-to-date, and, most importantly, exhaustive across everyone in your organization.

User Subtypes

Unlike in previous versions of SharePoint, in SharePoint 2010 you can have more than one type of User Profile, through the use of User Subtypes. A User Subtype essentially consists of a subset of all the default and custom-defined user properties. You can define as many User Subtypes as necessary to meet your needs, which lets you store different data about different types of people.

All out-of-the-box and custom properties are initially assigned to all User Subtypes. The User Subtype that's defined out of the box is called the Default User Profile Subtype. This means that when you create a new User Subtype, all existing properties are automatically assigned to it. You must then remove any existing properties that you don't want assigned.

As you create new properties, you can select which existing User Subtypes the properties should apply to; the Default User Profile Subtype is automatically selected by default. As an example, you might decide to add a new User Subtype for part-time employees, then add a new property that holds those employees' working days. You'd then apply the new property only to the part-time employees subtype.

The User Subtype is essentially used as a filter to determine which properties to display because, technically, all User Profile properties are actually associated with every entry in the User Profile. This means that if you change the User Subtype that a User Profile entry is linked with, then change it back again, the original properties associated with the User Subtype will retain their original values. This clearly must be the case if user properties can be associated with more than one User Subtype.

Properties and Attributes

As you create custom user properties (or modify default properties) through the Manage User Properties option, you need to consider the attributes to be applied to the property. These attributes control where and how the user property is used.

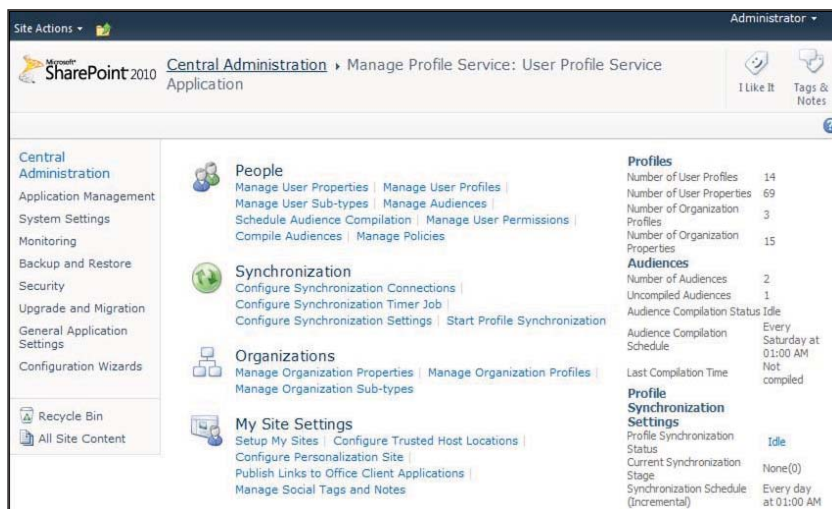


Figure 1: User Profile Service management

The Type attribute defines the type of data that the user property will hold. There are many valid data types, including text, dates, and person. The person data type requires that any data associated with the property be a link to another User Profile.

The Term Set attribute leverages the new Managed Metadata service and ensures that the data in the property is consistent. As an example, you could create a term set that contained the days of the week to hold the possible values for the part-time employee scenario described earlier.

Policy settings control how the property is used in terms of whether it requires a value, whether the user can override the value, and its privacy setting. (I'll discuss the effect of privacy settings in the third article in this series.)

Privacy settings control who is allowed to see the property. These settings can be set to one of the following values:

- Only Me
- My Manager
- My Team
- My Colleagues
- Everyone

Another policy setting determines whether a property is replicable (i.e., whether its value will be replicated to the user details that are held in site collections, such as team sites, blogs, etc., defined in the SharePoint farm). A property can replicate only if the user isn't allowed to override its value (to avoid inconsistencies) and if its privacy policy is set to Everyone (because there's no ability to limit who can see user details in a site collection).

Display settings control where a property is displayed. One interesting setting that I'll cover in the third article in this series is the ability to display updates to the property value in a user's newsfeed. (A newsfeed is like an RSS subscription to user activities so that you can follow what other people are up to.)

Synchronization settings control whether a property is mapped to an external data source for import and export purposes. I'll cover synchronization settings in the second article in the series.

Options for Populating the User Profile

Various methods are available to initially populate the User Profile. The method

you decide to use depends on the size of your organization and whether you have some other people directories deployed that might contain definitive information.

You can manually add User Profiles through Central Administration, or they can be dynamically created when suitably permissioned users access their My Site for the first time. As I mentioned, other options include populating the profile programmatically via the object model or the User Profile Service web service. You can also populate the profile through synchronization with AD (which I'll cover in part two of this three-part series) and other LDAP-compliant repositories, as well as external sources using BCS.



InstantDoc ID 129949



Kevin Laahs

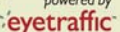
(kevin.laahs@hp.com) is a technology strategist with HP Enterprise Services. He's coauthor of four books on SharePoint; the latest is *Microsoft SharePoint 2010 All-in-One For Dummies* (Wiley).

Do you know what is being said
about your company online?

We do.  Do you have
time to warm prospects towards

a sale? We do.   

Announcing, smart marketing
for the technology industry. We
target the tough questions. 

 Penton Marketing Services™
WE KNOW YOUR CUSTOMERS powered by


Penton Marketing Services offers a full range of marketing products that leverage our deep industry knowledge and customer relationships. From product launch to the final sale – put our years of experience to work for you.

FOR MORE INFORMATION:
PentonMarketingServices.com
800 553 1945

NEW & IMPROVED

- Interoperability
- Backup and Recovery

- Application Management
- Security

Lenovo Releases New Workstation and Desktop Engines

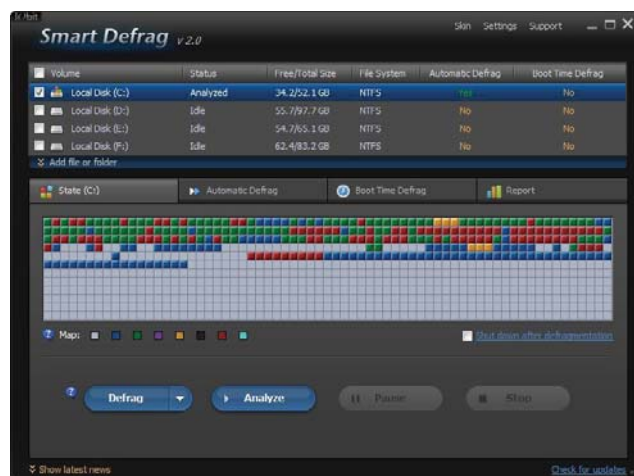
Lenovo has announced the **ThinkStation E30 workstation** and **ThinkCentre M81 desktop**, two new solutions that bring users speedy performance with second-generation Intel Core processors, rapid boot up/shut down, and extra productivity features. The E30 workstation is designed for creative, engineering, and financial professionals running specialized software. It offers 80GB or 160GB SSD storage, NVIDIA Quadro or NVS graphics, SATA III, USB 3.0, and 16GB of 1333 mHz error correcting code memory. The E30 starts at \$599. The M81 desktop has 160GB SSD storage, the choice of Intel HD graphics or ATI discrete Radeon graphics, SATA III, USB 3.0, and the potential to drive four independent displays by adding a discrete graphics card. The M81 starts at \$629. To learn more, visit www.lenovo.com.

IObit Releases Smart Defrag 2

IObit announced a new version of the free disk defragmentation solution

Smart Defrag 2.

The latest version offers a new UI, a "boot-time defrag" feature, and an improved defrag engine. Smart Defrag 2 can defrag files during the system boot process, which works well with files that cannot be defragged or are risky to move after the system is running. The product can also place frequently used files and directories into the fastest area of the disk, so your computer can run those files at top speed.



To learn more, visit www.iobit.com/iobitsmartdefrag.html.

Elevate User Privileges with Privilege Authority

ScriptLogic has released a new product called **Privilege Authority Professional** that lets IT administrators elevate user privileges to perform needed actions without having to establish the user as a local administrator on their PCs. Privilege Authority Professional works with Active Directory to centrally manage and automate the elevation of privileges for Windows PCs, based on least-privilege best practices. IT administrators retain complete control over PC administrative rights while providing end users specific and limited privileges so they can change computer settings or other configurations necessary for important day-to-day activities. To learn more, visit www.scriptlogic.com.

Cofio Releases AIMstor 2.3

Cofio Software has released **AIMstor 2.3**, the latest update to its backup and recovery solution. One key differentiator for AIMstor is that in addition to backup and recovery, the solution offers deduplication as well, promising to reduce data sprawl. Features include: secure connections between all distributed AIMstor nodes using Open SSL, firewall friendly for remote offices and workers, "cloud ready" for object storage of archived files and

PRODUCT SPOTLIGHT

Centrify Announces Centrify Suite 2011

Centrify has announced **Centrify Suite 2011**, which includes enhanced administration and privilege management for UNIX, Linux, and Mac systems; Group Policy support for GNOME desktops; enterprise-hardened DNS capabilities; and expanded platform support.

One key enhancement to the suite is Deployment Manager 1.2, which automates deployment of Centrify Suite on UNIX, Linux, and Mac systems. "With the new Version 1.2 release of Deployment Manager, you can now centrally manage local accounts and groups on systems discovered through DirectManage, whether those systems have been joined to Active Directory or not," wrote Tom Kemp, Centrify CEO, on his blog.

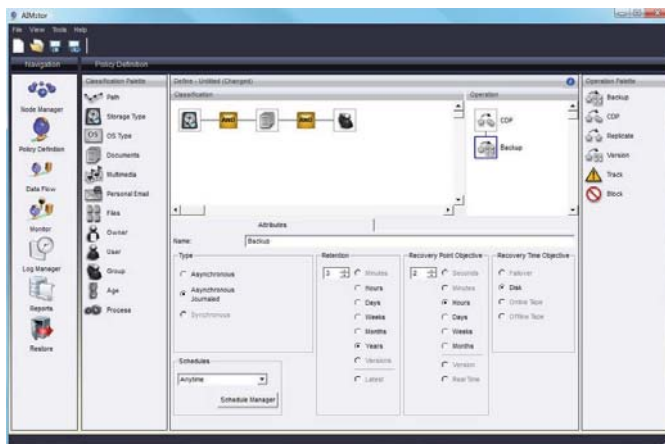
Centrify Suite is an interoperability product that lets you centrally manage and

secure an environment with a variety of client OSs. Products within the suite include DirectControl, which controls who can log in where; DirectAuthorize, which controls how and when users can log into UNIX and Linux; DirectAudit, which captures and reports on what users do on UNIX and Linux systems; DirectSecure, which provides end-to-end encryption; and DirectManage, which integrates with Active Directory.

"Centrify Suite 2011 boasts enhanced administration and privilege management capabilities for UNIX/Linux/Mac systems, expanded platform coverage and additional application single sign-on capabilities, allowing enterprises finer grain control and auditing over an expanded set of data center systems and enterprise applications," Kemp said.

To learn more, visit www.centrify.com.

NEW & IMPROVED



versions with set API, and real-time statistics of repository conditions and activities for snapshots and data transfers. The product also supports SQL and Exchange backup and replication. To learn more, visit www.cofio.com.

NopSec Enhances Risk Management Solution

NopSec has added two new modules (Web Application Assessment module and Internal Assessment module) to **VRM**, its vulnerability risk management solution. The Web Application Assessment module identifies security vulnerabilities and mis-configurations in the organization's web application infrastructure, protecting business and customer information. The Internal Network Assessment module lets organizations perform security assessments inside the organization through an easy-to-install hardware or virtual scanning appliance. The scanning appliance connects back to the NopSec VRM customer instance in the cloud, letting you remotely control the scan happening in the internal network. To learn more, visit www.nopsec.com.

App-DNA Releases AppTitude Application Management

App-DNA has announced **AppTitude 5.0**, a solution for managing and deploying applications. The product will determine the readiness of your applications to migrate to updated versions. According to the vendor, AppTitude automatically packages all applications (vendor supplied and in-house) that are ready for a new platform, and walks administrators through



a 'guided remediation' process for the rest. AppTitude 5.0 integrates with Microsoft System Center Configuration Manager and Active Directory. To learn more, visit www.app-dna.com.

Intellinet Unveils Wireless 450N Dual-Band Gigabit Router

Intellinet Network Solutions unveiled the **Wireless 450N Dual-Band Gigabit Router**. Built to meet the wireless networking needs of small to medium-sized businesses and high-demand home networks, the Wireless 450N delivers data, IP voice, HD video, and real-time audio/video streaming to any type of Wi-Fi enabled device at 450 Mbps. Intellinet has also enhanced the router to increase signal range and provide a more stable, reliable network. The router offers dual-band transceivers so the user can manage traffic between 2.4 GHz and 5 GHz bands. To learn more, visit www.intellinet-network.com.



Paul's Picks

www.winsupersite.com



SUMMARIES of in-depth product reviews on Paul Thurrott's SuperSite for Windows

Windows Phone 7 "NoDo" Update

PROS: Copy and paste; faster application start and resume; better Marketplace search

CONS: Slow time to market; inconsistent roll-out due to wireless carrier blocking; doesn't fix most of Windows Phone's shortcomings

RATING: ♦♦♦♦♦

RECOMMENDATION: When Microsoft delivered a buggy and incomplete Windows Phone 7 in late 2010, it seemed like the right thing to do: Get the product to market, then iterate on updates. Instead Microsoft will deliver just two notable software updates for Windows Phone in calendar year 2011. The first, code-named "NoDo," was delayed for months while the company's wireless carrier partners got around to OK'ing the release. It comes with just broadly useful changes: A limited form of copy and paste, faster application start and resume times, and better searching capabilities in Windows Phone Marketplace. But it doesn't fix the problems and missing features in Windows Phone.

CONTACT: Microsoft • www.windowsphone.com

DISCUSSION: www.winsupersite.com/article/windows-phone-7/windows-phone-7-nodo-135875

Apple MacBook Air (Late 2010)

PROS: One of the thinnest and most elegant 13-inch notebooks anywhere; instant resume

CONS: Price; installing Windows costs extra

RATING: ♦♦♦♦♦ (Three out of five stars with Windows 7)

RECOMMENDATION: Apple unveiled its second-generation MacBook Air notebooks in late 2010, in both 11.6-inch and 13.3-inch variants, and there's a lot to like: Quick boots and instant resume, surprisingly solid performance despite aging Core 2 Duo processors, the crazy-thin and crazy-light and elegant form factor. And the decent battery life, about six to seven hours for the 13-inch version. But it runs Mac OS X, which is less than ideal in corporate environments. So I tested various ways of installing Windows 7 on the machine: via virtualization, through a dual boot, and as the only OS on the Air. In that last configuration, the Air is a decent Windows machine.

CONTACT: Apple • apple.com/macbookair

DISCUSSION: www.winsupersite.com/article/windows-7/macbook-air-windows-7-part-worlds-135947

REVIEW

System Mechanic Business 10

Keeping your computer in top shape is important—doubly so when you're responsible for managing multiple computers across a company division, or even an entire enterprise. Many products in the industry claim to fix everything that ails your computer. Some tout incredible performance increases, using marketing materials that show users beaming beside their computers because the miracle product has cured all their problems. I recently tested System Mechanic Business 10 from Iolo Technologies to see how it performed against the company's claim to "fix and speed up your PC . . . automatically!"

I had my choice of OS to work with, because the product is compatible with Windows 7, Windows Vista, Windows XP, and Windows Server 2003. Initially I planned to install the software on a Windows 7 machine, but I wanted to give the product a really thorough workout, so I downloaded and installed it on a 2-year-old test laptop: a Lenovo ThinkPad T61 running XP SP3. The system was working well, but because of its age and the myriad of software that had been installed on it and uninstalled from it during testing, I assumed that System Mechanic would be able to find and fix more errors and problems on this system than on, say, an out-of-the-box factory-fresh PC.

The executable file that I downloaded from Iolo's website didn't install the product directly. Instead, it let me create a customized Windows Installer file with various installation options already set (e.g., product key, file paths to install to). This .msi file can then be deployed to user desktops using Group Policy Software Installation (GPSI) or another tool, such as Microsoft System Center Configuration Manager (SCCM). Being able to build a Windows Installer file in this fashion is a nice touch; however, there's currently no way to change any of the settings after the product is deployed, aside from building a new .msi file with the deployment tool. An Iolo representative told me that improvements to this process are in the development pipeline.

The customized Windows Installer file that I created consisted of no changes other than adding the product key Iolo provided for the review. When I ran the .msi file, the product installed quickly and successfully. Eager to see what the product would do for my aging laptop, I started the software and was greeted with a colorful interface stating that I should analyze my system.

The initial analysis completed quickly, informing me that I had "7 problems and 1 warning." I was offered two options: Repair all the problems or view them. I wanted to see exactly what problems the software found before I made any changes, so I selected the option to view the problems. At first glance, this option provided only a high-level overview of the problems found, such as "4 Registry problems." What I wanted was a detailed list that I could quickly review before I made any changes, but I could find no way to get such a report. Stymied, I reluctantly told the software to fix all the problems it found, hoping I would be provided with a report later on that showed me exactly what was found and what was fixed.

To my surprise, this didn't happen either. Confused, I searched through the UI until I came to the SafetyNet area, where I found an option to export a list of the changes made to an XML file. Then, by examining the XML, I was able to finally determine what the product had done. However, fixing the Registry "problems" the software found (related to JavaScript shell handlers and DirectShow filters) didn't make my test computer any faster. On the plus side, these changes also didn't make the computer any slower or cause any other problems.

To make sure that I hadn't missed an option somewhere, I contacted Iolo to ask if this was indeed the process to find out exactly what changes the software would like to make to a system. Fortunately, it isn't—but the correct process

isn't nearly as well-defined as it should be. After the software completes a system analysis and you select the View Problems option, each problem area (e.g., "4 Registry problems") is identified. Each problem area also has a Repair option and a drop-down arrow that exposes additional options, such as the wizard option. For a registry problem, for example, you can select *Start Registry Repair wizard*. Descriptive text states that the wizard can be used to "inspect and repair the problems yourself." Likewise, selecting the Repair option presents two additional options: *Repair Now* and *Inspect problem*. The heading next to the *Inspect problem* option states: "Resolve problem using advanced options." The *Inspect problem* option subsequently launches the repair wizard.

The first time I explored the software, I didn't notice either of these options, primarily because the heading text isn't descriptive enough. I did click the drop-down arrow and saw the *Start Registry Repair wizard* choice, but my thinking was, "I don't want to run a wizard; I just want to see a list of the problems"—so I ignored it. Likewise, blindly clicking the Repair option was the last thing I wanted to do. To me, "Repair" suggests that the problem will be repaired immediately, not that you'll be presented with two additional options. Furthermore, what if clicking the Repair option merely performed the repair without any confirmation whatsoever? The software desperately needs a way for users to view a detailed list of the problems found, including recommended fixes, as soon as an analysis is completed.

I explored the rest of the UI and saw such interesting items as the ability to speed up my Internet connection and remove unneeded startup services. I ran the Internet speed optimizer, which apparently modifies items such as the Maximum Transmission Unit (MTU) on your Ethernet adapters—but I didn't



Michael Dragone | articles@mikerochip.com

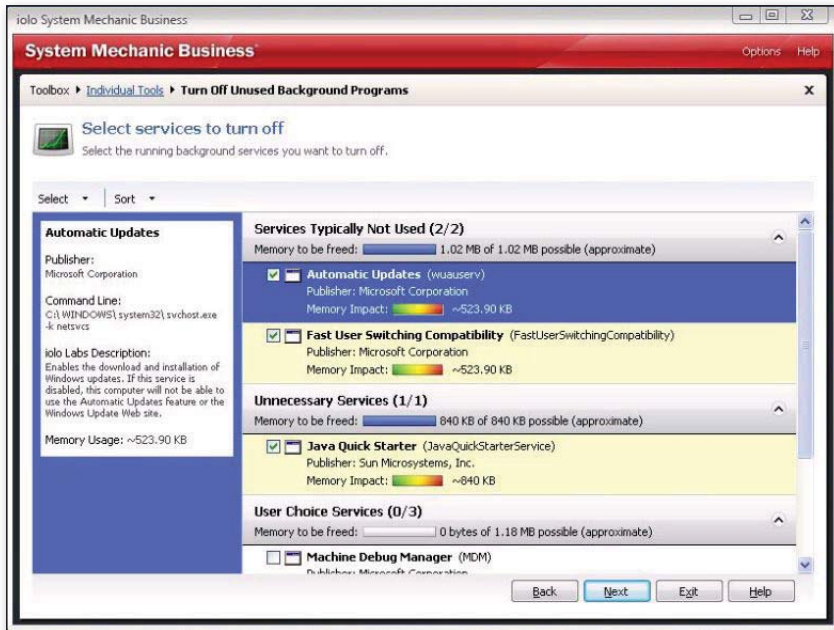


Figure 1: List of services System Mechanic recommended to disable

notice any increase or decrease in perceived Internet speed. I ran the tool that identifies and offers to remove unneeded startup services, and I was likewise disappointed. The first service the tool identified as “typically not used” was the Windows Automatic Update Service, as Figure 1 shows. The software also includes the ability to tweak various parts of the Windows shell, just like the TweakUI PowerToy that Microsoft offers as a free download.

The reporting that System Mechanic Business provides is mediocre, offering only a high-level history view, as Figure 2 shows. I searched in vain for a way to export or email reports. Likewise, there’s no centralized management console that you can deploy and use to monitor systems that System Mechanic is installed on and generate reports or approve or deny potential changes. According to Iolo, both report exporting and emailing capabilities and a centralized

management console are in the development pipeline, to be included in a future release.

In its current form, System Mechanic Business is perhaps best suited to the small business owner who is “unofficial IT” and who isn’t interested in the nitty-gritty of what changes the software is making as long as he is able to undo what was done if there’s a problem. Unfortunately, it’s unlikely that the owner of a small-to-mid-sized business (SMB) will have the technical skill set to build a Windows Installer file using the included tool, let alone deploy it using Group Policy or another method. An SMB owner might also take the product’s “advice” and disable a service such as Automatic Updates—something that definitely wouldn’t be a good move even if the user didn’t recognize it as a poor decision.

For enterprises, System Mechanic’s lack of quality reporting and a centralized management console are huge barriers to adoption. However, because of the controlled nature of most enterprise environments, the need for tune-up software such as this is typically low.

Overall, System Mechanic Business is extraneous for nearly everyone. The parts of the software that are worthwhile are easily handled by other (typically free) utilities. Combining these tools into one piece of software is the product’s greatest strength; however, the product’s weaknesses severely outweigh its lone benefit.

InstantDoc ID 130018

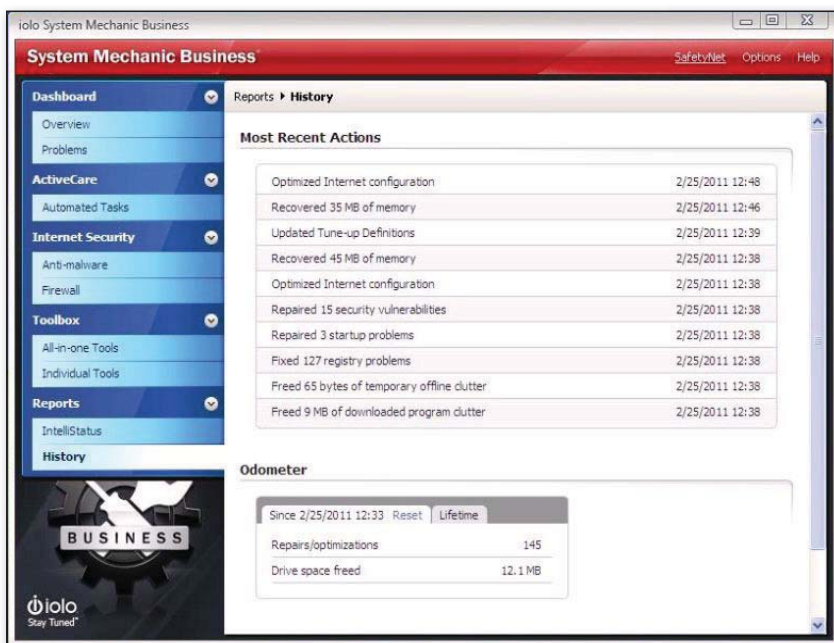


Figure 2: System Mechanic’s high-level reporting

System Mechanic Business 10

PROS: Inexpensive; combines the functionality of many separate tools into one

CONS: Included tools are available elsewhere for free; lacks a centralized management console and detailed reporting; UI text is misleading

RATING: ◆◆◆◆◆

PRICE: Starting at \$79 for up to five PCs with 1 year of included updates

RECOMMENDATION: Consider this product only if you have a burning need for the functionality it provides and you can live with its serious shortcomings.

CONTACT: Iolo Technologies • 323-257-8888 • www.iolo.com

Mac-to-AD Integration Solutions

Manage your Apple Macintosh clients like you manage your Windows clients

by Eric B. Rux

It wasn't too long ago that using an Apple Macintosh computer in a Windows environment meant hassling with software integration and Active Directory (AD) schema changes. Within the past few years, however, this integration has become a lot easier and literally out of the box. This change didn't occur because Microsoft and Apple suddenly had a kumbaya moment and started working together. It occurred because they both have done a great job of following the RFC 2703 and LDAP standards. As a result, if you're using Windows Server 2003 R2 or later and Apple OS X Panther (version 10.3) or later and you just need your Mac clients to authenticate to AD, you don't need any special software. You can simply specify the old "NT style" Home Folder path in the user's AD object to have the user's network drive show up on the desktop. If it's a mobile account (what Microsoft calls "cached credentials and a Profile"), users can even log on when they aren't connected to the domain—again all without any additional software. But if you want to manage your Mac clients like you manage your Windows clients, you'll need a Mac-to-AD integration solution. I recently reviewed four products that do a great job.

Three of the products—Centrify's DirectControl, Likewise Software's Likewise Enterprise, and Quest Software's Authentication Services—integrate Mac, UNIX, and Linux computers into your Windows world. The fourth product, Thursby's ADmitMac, integrates Mac computers only.

Product Testing

I tested each product in a dedicated Windows Server 2008 AD environment hosted on a VMware ESXi server. I installed DirectControl and Authentication Services directly on the domain controller (DC). As recommended by the documentation, I installed Likewise Enterprise on a dedicated server. ADmitMac doesn't require the installation of back-end software.

For the client, I used a MacBook Pro running OS X Snow Leopard (version 10.6.7). After installing and configuring each product, I ran it through the paces. The testing involved:

- Installing the client software
- Adding the Mac client to the domain
- Removing the Mac client from the domain
- Logging on to the domain
- Migrating a user

- Using the product's management console (if applicable)
- Changing settings using a Group Policy Object (GPO)
- Adding a Global Group to a Local Group
- Deploying software to the Mac client
- Using cached credentials to log on when not connected to the domain
- Disabling automatic logons and logon messages using a GPO

For more information about the testing, see the web-exclusive sidebar "Criteria for Testing the Mac-to-AD Integration Solutions" (www.windowsitpro.com, InstantDoc ID 135957).

DirectControl

Installing DirectControl is a breeze. You simply double-click *CentrifyDC_Console-4.4.3-win32* on a DC and follow the prompts. No database or other prerequisites are required, except to disable the *.Net Publisher evidence verification* option. Disabling this feature is easy, as the installation routine does it for you. However, finding out what the *.Net Publisher evidence verification* option proved to be a bit more challenging. After numerous Internet searches and queries to my developer friends, I finally reached out to the folks at Centrify for an explanation. According to Centrify, "Disabling the 'publisher evidence verification' simply speeds up the launch of the console applications since it configures the app to launch without performing the time-consuming verification process, which can be problematic in isolated networks such as test labs that don't have Internet connectivity."

After the setup routine finishes, you start the DirectControl console. The first time this program runs, a setup wizard walks you through setting up the default zone. Zones help you collect and identify collections of UNIX, Linux, and Mac computers. By grouping the client machines this way, you can easily enforce security or configuration policies. Zones are stored in the AD container `domain.com/Program Data/Centrify/Zones`.

The setup wizard also helps you install the required licenses, which are stored in the AD container `domain.com/Program Data/Centrify/Licenses`. In all of the products that I've reviewed, I've never seen licenses stored in AD. It's unique, to say the least.

After the back-end support has been installed, the next step is to install the client software onto a Mac computer using a platform-specific package. For Mac OS X Snow Leopard, you

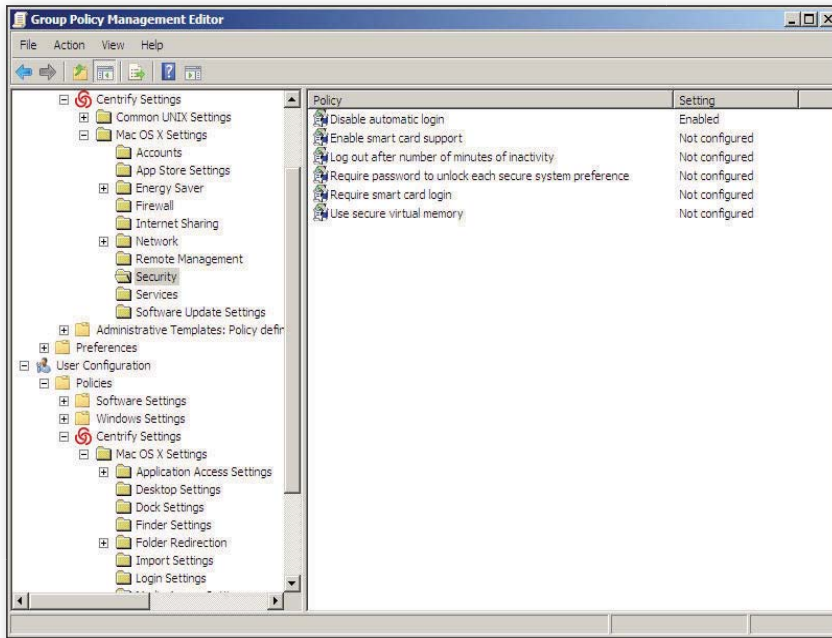


Figure 1: DirectControl's integration into GPMC

use the CentrifyDC-4.4.3-mac10.6.dmg file. Double-clicking this file opens a menu that has a Prepare feature, which you use to ensure that DirectControl and AD are communicating properly and ready for integration. When prompted, you enter the name of your domain, and in a few seconds, a total of 20 tests are performed. These tests check to see whether there's adequate disk space on the client, whether DNS is working properly, whether there's a DC in the site, and much more. I failed the test that checked whether the DC's and the client's clocks were synchronized. After I fixed the problem, I was ready to install the client.

The installation itself takes only a few seconds, then DirectControl prompts you to join the domain. I like this feature, as it takes away any confusion about when you need to add the machine to the domain. From the configuration screen, you can set the user's home directory (/home/username), UNIX ID, and group ID, or you can let DirectControl's Auto Zone mode configure them for you. Manually configuring the UNIX ID and group ID is important if you're integrating a UNIX or Linux machine but since I was integrating a Mac machine, I chose the Auto Zone mode. It worked fine. (For more information about UNIX IDs and group IDs, see "Cross-Platform Identity Management Solutions for Single Sign-On," September 2007, InstantDoc ID 96592.)

The logging that's produced from the configuration screen is extremely helpful. I accidentally misspelled the domain's name and the log was very helpful in troubleshooting the problem. Rebooting is recommended after you join the computer to the domain.

After the MacBook Pro rebooted, I successfully logged on as a domain user. I didn't have to add *domain* to the beginning of the username or add *@domain* to the end of the username. Because it was the first time I logged on with that account, I was prompted to change the password. After I did so, the logon process continued.

Credential caching worked right out of the box. To test this feature, I unplugged the network cable, disabled the AirPort network card, then logged off. When I attempted to log on, my cached credentials were used and I was soon looking at the desktop again.

Back on the DC, I found a new Centrify Profile tab on the user object and computer object properties pages in the Active Directory Users and Computers snap-in. On the computer object properties page, this tab contained read-only information, such as the version of the client software, the type of zone being used (Auto Zone, in my case), and whether the client was using licensed or unlicensed features. On the user object properties page, this tab contained configurable information. Although doing so

isn't necessary for integrating Macs into an AD domain, you can configure some UNIX and Linux settings, such as the UNIX ID, logon name, Shell (/bin/bash), home directory, and primary group.

DirectControl is tightly integrated into the Group Policy Management Console (GPMC). As Figure 1 shows, you can easily manage your Mac clients. For example, I disabled automatic logons. As with a Windows machine, you can configure an OS X computer to log on automatically. However, unlike a Windows machine, this functionality isn't disabled when the computer is joined to the domain. If a user knows the local machine's administrator password, he or she can easily configure the machine to start up without a password credential. With just a few clicks, I was able to disable this feature.

DirectControl offers a handy Mac utility named the DirectControl Widget. It displays information about AD's status, Kerberos, AD accounts, and AD group membership. To install this widget on a Mac computer, click Go, select iDisk, click Other User's Public Folder, enter Centrify, and double-click DirectControl Widget.

Centrify DirectControl

PROS: Great support for Mac, UNIX, and Linux clients

CONS: Zone concept can be confusing and might not be necessary for smaller deployments

RATING: 

PRICE: Starts at \$60 per workstation (volume discounts available)

RECOMMENDATION: If your UNIX or Linux clients are currently using different methods to authenticate and you need to keep your UNIX IDs and group IDs straight, DirectControl's zone technology and attractive price might push it to the top of your list.

CONTACT: Centrify • 408-542-7500 • www.centrify.com

Likewise Enterprise

The installation guide makes it very clear that you shouldn't install Likewise Enterprise directly on a DC. Instead, the guide recommends installing it on a dedicated server running Windows Server 2008. Alternatively, you can install it on a computer running Windows 7, Windows Vista, or Windows XP. Likewise Enterprise enhances

■ MAC-TO-AD INTEGRATION

the built-in AD administration tools (i.e., GPMC and Active Directory Users and Computers snap-in), so these tools must be already on the computer in which you install Likewise Enterprise. Microsoft Management Console (MMC) 3.0 is also required. Because you can't install MMC 3.0 on Windows 2000, you can't install Likewise Enterprise on Windows 2000 Server.

After Likewise Enterprise is installed, a wizard walks you through the setup process, including picking a mode and setting up a cell in AD. I found the wizard to be a bit confusing and had to read and reread the PDF manual to understand what it was trying to accomplish.

Picking a mode. Both my forest and domain were running at the Server 2008 functional level, yet the wizard was trying to steer me to use its Non-Schema Mode—the mode that supports Windows 2000 AD. (If you're running Windows 2000 AD, you'd have to run Likewise Enterprise on XP or later and extend the schema.) In addition, the instructions in the wizard are incomplete, but I figured it out. To use Schema Mode—the mode in which Likewise Enterprise takes advantage of RFC 2307—you have to cancel the wizard and run a separate Schema Mode Wizard, which you'll find by navigating to Console, Enterprise Console, Status. Even with the forest and domain running at the Server 2008 functional level, the wizard ensures that certain attributes (e.g., uid, uidNumber, gidNumber) are indexed and present in the AD Global Catalog (GC).

Whether you use Schema Mode versus Non-schema Mode depends on what OS your domain is running. If it's running Windows 2003 R2 or later, no schema changes need be made to your domain so you should use the Schema Mode. If your domain is running an earlier OS, you have two options. You can use Non-Schema Mode and store the group or user information in the multivalued *keywords* and *description* attributes of the user and computer objects. Or, if you're feeling especially brave, you can have Likewise Enterprise extend the schema for you.

Setting up a cell. Like DirectControl's zones, Likewise Enterprise's cells let you logically group non-Windows machines and control their information (e.g., UNIX ID, group ID). Also like zones, cells are logically connected to OUs. Using this structure,

you can create a cell for each department or security boundary in your company and assign a user to one or more cells using the Likewise Settings tab in the Active Directory Users and Computers snap-in.

After the server software is installed and configured, it's time to install the client software on each Mac computer. You can manually install it with the installation CD-ROM, or you can install it through an unattended installation that uses Secure Shell (SSH). (Apple's name for SSH is Remote Login, which you can enable in System Preferences, Sharing.) The PDF manual gives a good walkthrough on how to install the client software using SSH.

Next, you need to join the computer to the domain using the Likewise—Active Directory tool, which is in the Directory Utility. Just like the built-in *Active Directory connector* that comes with OS X, the Likewise—Active Directory tool lets you choose which container or organizational unit (OU) to create the computer object in.

Likewise Enterprise is tightly integrated with Group Policy. Figure 2 shows how easy it is to configure local administration privileges for a domain user or group.

If you have an infrastructure in place for Mac authentication and you want to migrate everything to AD, Likewise Enterprise offers a migration tool that imports Mac, UNIX, and Linux passwords and group files. These attributes are automatically mapped to users and groups in AD.

If your environment uses local authentication and has OS X user profiles established, you might want to migrate them to the new domain authenticated account. For example, suppose that John has been using his MacBook Pro for a year and you now want him to authenticate to the domain. Just like a Windows machine, the OS X machine will create a new profile the first time he logs on. The Migrate User Profile tool moves the old local profile to the new domain-based profile. When John logs on to the domain with his new account, he'll see the desktop that he's used to.

Likewise Software Likewise Enterprise

PROS: Great support for Mac, UNIX, and Linux clients

CONS: Cell concept can be confusing and might not be necessary for smaller deployments; Non-Schema Mode versus Schema Mode isn't intuitive during the setup process

RATING: ◆◆◆◆◆

PRICE: \$69 per workstation (volume discounts for quantities of 50 or more)

RECOMMENDATION: If your UNIX or Linux clients are currently using different methods to authenticate and you need to keep your UNIX IDs and group IDs straight, you might find that you need Likewise Enterprise's cells.

CONTACT: Likewise Software • 425-378-7887 or 800-378-1330 • www.likewise.com

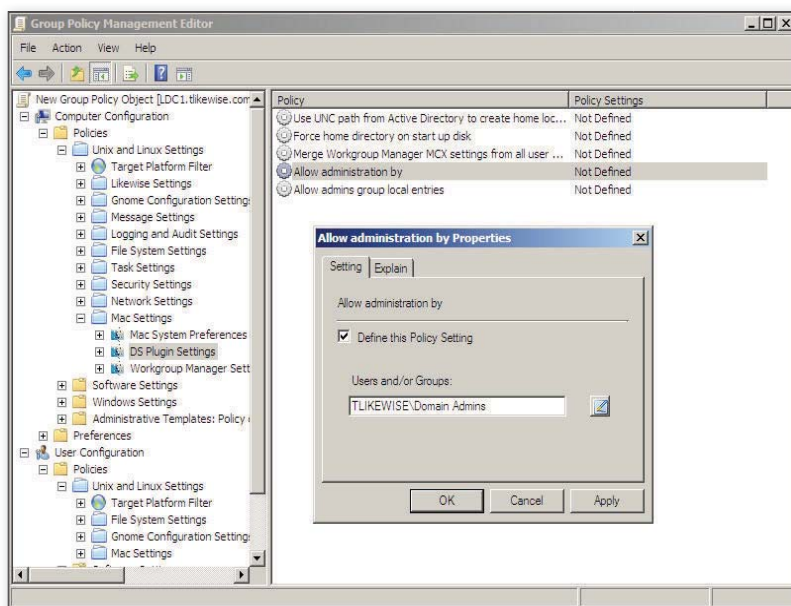


Figure 2: Likewise Enterprise's integration into GPMC

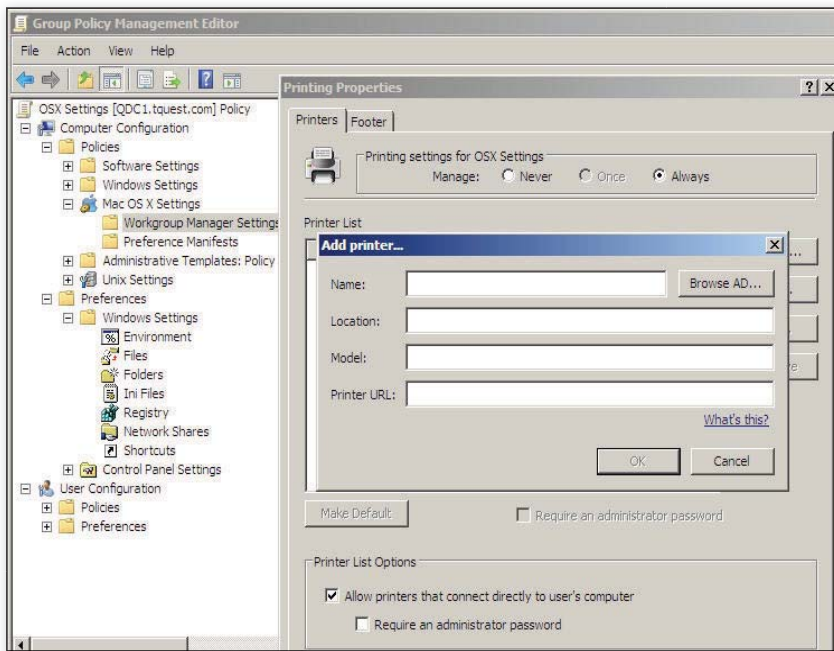


Figure 3: Authentication Services' integration into GPMC

Authentication Services

Authentication Services requires that Microsoft .NET Framework 3.5 SP1 and Windows PowerShell be installed. Authentication Services' installation process will install (and even help you download) all required components. The installation process will also verify that your AD schema will support the product. As with the other software discussed here, as long as you're using Windows 2003 R2 or later, no schema extensions are required.

Unlike DirectControl and Likewise Enterprise, Authentication Services doesn't use zones or cells. Thus, the product is very simple to set up. The *Add and Join Host* wizard walks you through the setup process, which involves:

- Adding and profiling hosts (aka clients). The server running Authentication Services must have name resolution to the Mac clients. The client should dynamically add itself to DNS, just like a Windows 2000 or later machine. However, I had mixed results. If you can't resolve the OS X host name, make sure that there's an *A* record for the client in DNS.
- Checking the clients for readiness to join AD. The AD Readiness check ensures that the client is ready to join the domain. In my case, I received an error message noting that the "time

skew" (i.e., the difference between the DC's time and the client's time) was too great, so the client couldn't be joined to the domain. I appreciated that the error message was clear and concise, unlike the built-in *Active Directory connector*, which provides cryptic messages.

- Installing the client software. When I attempted to install the client software, an error message stated that Authentication Services couldn't find the client for Mac OS X 10.6. I checked the path that was provided, and sure enough, the client file (VAS-4.0.1.52.dmg) was missing. After I downloaded VAS-4.0.1.52.dmg and copied it to the source directory, the installation finished without any further problems.
- Joining the clients to AD. Joining a client to a domain requires a root or administrator password.

I really liked the *Add and Join Host* wizard. As long as the Mac client is running SSH, you can add the client to the domain without ever leaving your desk.

After the client has been added and joined to AD, there isn't a whole lot to do with the Authentication Services-specific tools that are provided. The real meat is in the functionality that the product adds to

GPMC, as Figure 3 shows. Adding printers is just one of the many features that you can manage within Group Policy.

To log on to a non-Windows machine, the AD user account has to be "UNIX-enabled" through a Quest tab on the user object properties page in the Active Directory Users and Computers snap-in. This creates the needed UNIX ID and group ID.

Overall, I found the Quest product to be easy to setup and use. If you have a mix of UNIX, Linux, and Mac clients, put Quest at the top of your evaluation list.

Quest Software Authentication Services

PROS: Automated client installation and domain join through a GUI; great support for Mac, UNIX, and Linux clients

CONS: Price

RATING: ◆◆◆◆◆

PRICE: \$37 per user and \$65 per computer

RECOMMENDATION: If you support a large Mac, UNIX, and Linux community, Authentication Services is the best choice. You can deploy the software from your desk and don't have to mess with complicated cell or zone concepts.

CONTACT: Quest Software • 800-306-9329 • www.quest.com

ADmitMac

ADmitMac has a much different architecture than the other three products, so I chose to review it last. What quickly set this product apart is that it's built solely for Mac integration into AD. The other products are UNIX- and Linux- centric, and the Mac support appears to be an afterthought. ADmitMac doesn't try to be anything other than a Mac-based product. This doesn't make ADmitMac any better or worse than the other three. If you're integrating a mix of UNIX, Linux, and Mac clients into your Windows environment, you'd be better off with one of the other three products reviewed. If you're integrating Mac clients only, you should first look at ADmitMac because its sole purpose is make Mac clients behave like Windows clients.

Instead of starting the installation on the server side like with the other products,

MAC-TO-AD INTEGRATION

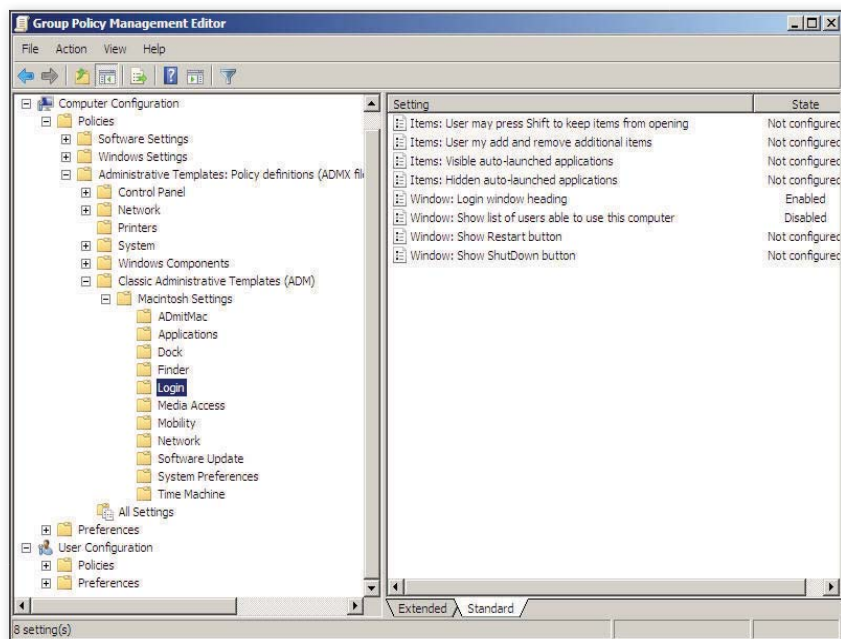


Figure 4: ADmitMac's integration into GPMC

ADmitMac installation starts on the client side. After you use the installation CD-ROM to install ADmitMac, the Setup Assistant (a wizard) walks you through configuring the ADmitMac networking software. The first screen is a bit of a surprise, as it asks for WINS information. You can either manually set the WINS information, or set it to DHCP.

The next screen sets the Security Policy Settings—whether the Mac client will use Kerberos, NTLMv2, NTLM, or LAN Manager to log on to the Windows domain. The default setting is to use NTLMv2 or Kerberos first, use NTLM next, and never use LM. You can set the ADmitMac client to send passwords in clear text, but you obviously must have another mechanism in place on the network to protect that information before you choose that option.

The next step is to add the Mac client to the domain. After you enter the domain's name, you're prompted for the network administrator username and password. You then specify where the machine account should be created in AD. The default location is the Computers container.

Finally, you set the type of Home Folder (i.e., Network, Local, or Mobile) that the user will use. You can also specify how many times a user can log on when not connected to the network.

That's all that needs to be done to get the Mac client added and connected to the domain. The ADmitMac directory utility has more features, though. Like the other products, ADmitMac lets you map UNIX IDs and group IDs to AD accounts, but this is done from the client side. You can also put OU restrictions in place. For example, if you enter *Sales* in the Users OU, only those user accounts located in the Sales OU would be able to log on to the computer.

Although ADmitMac is managed from the server side, there's no software to install. Instead, it uses Group Policy .adm files, as Figure 4 shows. Because the files don't use the new .admx format, they're buried a bit in the Server 2008 GPMC. However, this doesn't take away from the fact that Group Policy support has been added to Mac clients with no additional software on the server—only .adm templates are added.

To add the templates, you run an executable (ThursbyADMInstaller.exe) that copies them from the installation CD-ROM to the DC. The default location is C:\Windows\inf. Once they're copied, you use these .adm templates just as you would any other template: Right-click Administrative Templates, select Add/Remove Templates, click Add again, and find the ADmitMac .adm template file.

Thursby Software ADmitMac

PROS: No back-end software to install in the data center

CONS: Mac clients only

RATING: ◆◆◆◆◆

PRICE: \$84 per computer for 250 seats, \$60 per computer for 500 seats (discounts available)

RECOMMENDATION: If you have only Mac clients, with no plans to incorporate UNIX or Linux clients, ADmitMac is the hands-down choice. The robust client and absence of back-end software make this the cleanest integration of OS X into AD that I've seen.

CONTACT: Thursby Software • 817-478-5070 • www.thursby.com



Editor's Choice

With DirectControl, Likewise Enterprise, Authentication Services, and ADmitMac, you can integrate and manage Mac clients in your AD domain. Each product provides easy domain logons, but so does the built-in *Active Directory connector* that comes with OS X. What sets these products apart is that they let you manage your Mac clients like you manage your Windows clients.

DirectControl and Likewise Enterprise are similar in how they work. Both let you logically group non-Windows objects together.

Quest stood out because it didn't require this additional overhead. In addition, you can use a central console to install the client software and add the client to the domain. This could be very important if you have a lot of Mac computers to migrate to AD.

ADmitMac emerged as the winner because this review focuses on Mac-to-AD integration solutions. For this task, it has a slight edge. ADmitMac doesn't require any special software on the server side, and the client software is full of added features. ◆

InstantDoc ID 135918



Eric B. Rux

(ebrux@whshelp.com), Windows Home Server MVP, is a contributing editor for *Windows IT Pro* and writes a monthly column at svconline.com/connectedhome/windowshomeserver. Eric is the manager of technical support services at Eastern Washington University.

SharePoint Migration

by Caroline von der Marwitz

Editor's Note: Information in this buyer's guide comes from vendor representatives and resources and has been edited for brevity. Every attempt at accuracy has been made, but errors in editing can still occur. Please contact individual vendors with any questions you might have about this content.

On the road to your SharePoint 2010 migration, you might need a little help with navigating the mind-numbing prerequisites and managing the sweat-inducing planning, fixing, and monitoring involved. Thanks to the experts who've documented the route, SharePoint migration seems almost a safe, predictable journey. Perhaps with the right guide it is: Besides the obvious TechNet resources (technet.microsoft.com/en-us/sharepoint/ee517214.aspx), we like

- Randy Williams on SharePoint 2010 migration (www.sharepointpromag.com/article/migration/migrating-to-sharepoint-2010.aspx)
- Joel Oleson on migration tools (www.sharepointjoel.com/Lists/Posts/Post.aspx?ID=337)
- Christian Buckley on a variety of migration topics (info.axceler.com/Blog/bid/51255/Understand-Your-SharePoint-Customizations-Before-Migrating)
- Anders Rask for his earnest and helpful account (sites.wizdim.com/andersrask/files/2010/05/WhitePaper-Upgrading-SharePoint-2007-to-SharePoint-2010.pdf)

Still, despite the reassurance of earlier travelers, you're setting off on the IT equivalent of a grand expedition to the edge of the previously-known-flat world, with all the details and prerequisites of a major journey. Before you even get started, you have to deal with the need for 64-bit architecture, as SharePoint 2010 is available only in 64-bit versions and requires Windows Server 2008 SP2 or R2. You also need to snag a 64-bit edition of Microsoft SQL Server, either SQL Server 2005 SP3, 2008 SP1, or 2008 R2. Not to mention that you need Microsoft .NET Framework 3.5 SP1 and just a couple other small things (<http://technet.microsoft.com/en-us/library/cc262485.aspx>).

Is it any wonder that you haven't migrated yet? But you know it's inevitable, once the funds and the approvals come in. And while many say that SharePoint 2010 is a great step forward, one must also acknowledge that it's different, for better or for worse, than what you and your users have previously experienced.

As you probably know, Microsoft left the door open to SharePoint migration vendors, especially for moving from SharePoint Portal Server (SPS) 2003 to SharePoint 2010. The two versions and their hardware requirements are far too different to allow for a direct, in-place upgrade. If you're into doing it yourself, you can hopscotch from SPS 2003 to Microsoft Office SharePoint Server (MOSS) 2007 to SharePoint 2010 by doing a series of database-attach upgrades. Even if you're simply looking to take your MOSS 2007 setup to SharePoint 2010, however, you've got a lot of work ahead of you. Which is why we've created this buyers' guide on SharePoint migration products, in case you're investigating other options.

If you've been involved with SharePoint for even a short time, you're aware of the big names in SharePoint products. They're well represented in the SharePoint migration arena, as well as some vendors you might not yet know. We can't presume to tell you which to choose. Our goal instead is this: To gather information about the SharePoint migration products that are most well known and present it as simply and cleanly as we can.

That process is admittedly unscientific, and some of the categories in the accompanying buyer's guide table might make you scratch your head. You might also see gaps where you need more information. And there is that matter of sifting through the marketing-speak to find the concrete facts. No single website answered all the questions, as you've probably found too. So we asked the vendors for additional information, which we edited for space.

That said, will one feature tip the scales for you in favor of one solution over another? We doubt it—a good fit involves a combination of features, plus such difficult-to-measure aspects as helpfulness and responsiveness of the solution provider's support techs. Solution vendors in general, though eager to say that *everything* is their strength, tend to know which of their product's features are the best. Each vendor thinks they've created the perfect iteration of features for SharePoint migration in their solution—and maybe they have—but the only way to find out if it's perfect for you is to do a trial. The product table will get you started.



InstantDoc ID 129994



CAROLINE VON DER MARWITZ

(cmarwitz@penton.com) is the editor of *SharePoint Pro* and also edits and writes for *Windows IT Pro* and *SQL Server Magazine*. She specializes in SharePoint but also covers Active Directory and Group Policy.

Company	Product	Price	Versions Migrated/ Migration Targets	Agentless, or Server-Side Install?	Migrates to Cloud/ Hosted?	Migrate Web Parts?	Migrate Workflows?	Migrate InfoPath Forms?	Migrate Term Stores?	
AvePoint www.avepoint.com	DocAve SharePoint Migrator for Microsoft SharePoint	Priced per gigabyte of content migrated and tiers off the more content being migrated; all licenses are perpetual; contact company for details	SharePoint Portal Server (SPS) 2003 (for Exchange public folders and SharePoint 2001); Windows SharePoint Services (WSS) 2.0; WSS 3.0; Microsoft Office SharePoint Server (MOSS) 2007; SharePoint 2010; Microsoft Exchange 2007/2010	Server-side install; however, agentless solution is available for migrations to SharePoint Online	Yes, with DocAve Website Migrator via web services can migrate to SharePoint Online and other hosted Microsoft SharePoint environments	Yes	Yes, for MOSS 2007 to SharePoint 2010 can migrate workflows (state, history, and definition) and SharePoint Designer workflows that don't write workflow data outside of parent list, task list, and history list	Yes	Yes, assuming mapping into term stores of existing metadata into SharePoint 2010 metadata terms/columns	
Axceler www.axceler.com	Davinci Migrator for SharePoint 2010	Pricing is based on number of Web Front Ends (WFEs) and the amount of data to be migrated; pricing starts at \$5,000	SPS 2003 and MOSS 2007 to SharePoint 2010	Server-side install	Yes, supports migrations to dedicated cloud environments; multi- tenant migration will be supported in a future release	Yes, out-of- the-box Web Parts, as well as most third- party ones (if instantiated on the destination system)	No, however support for workflow migration is targeted for the next release	No, however support for InfoPath forms is targeted for the next release	Can migrate custom content types; doesn't currently support migrations between 2010 farms but will in a future release	
Idera www.idera.com	SharePoint migration manager	\$5,995 per seat	Migrates across or within SPS 2003, MOSS 2007, SharePoint 2010, and Microsoft Business Productivity Online Suite (BPOS)	Agentless; supports SharePoint web services	Yes, supports BPOS and other hosted SharePoint providers	Yes	Yes	Yes	Yes	
Metalogix www.metalogix.com	SharePoint Site Migration Manager 2010	Offers flexible licensing and pricing options based on capacity or WFEs; contact company for details	SPS 2003 and MOSS 2007 to SharePoint 2010	Agentless; supports SharePoint web services; optional web service install on server for added functionality	Yes, can upgrade from SharePoint 2003, SharePoint 2007, or SharePoint 2010 to BPOS-D with Metalogix SharePoint Site Migration Manager for BPOS-D	Yes, can migrate Web Parts; third-party Web Parts must be manually installed on the target before migration	No, however added support for workflow associations, limited support for templates, and working on more features (e.g., instances)	Yes	Term stores are new to SharePoint 2010, and no one has asked us to migrate them yet	
MetaVis Technologies www.metavistech.com	MetaVis Migrator for SharePoint	Pricing options start at \$2,500; contact company for details	SPS 2003, MOSS 2007, other SharePoint 2010 (including 2010 beta) sites and file system network shares to SharePoint 2010	Agentless	Yes, with MetaVis Migrator for Office 365 can migrate to Office 365 from SharePoint 2010 (on-premises or hosted); SharePoint 2007 (on-premises or hosted); SharePoint 2003 (on-premises or hosted); BPOS (S or D); file systems; Outlook; Exchange public folders; cloud to cloud	Yes	Yes	Yes	Yes	
Quest Software www.quest.com	Migration Manager for SharePoint	Contact company for details	MOSS 2007, SharePoint 2010	Server-side install	Planned for Q3 2011	Yes, enables Web Part page migration including layout and Web Parts	Yes, SharePoint Designer workflows	Yes	No	
Synergy www.synergy.com	Connect for SharePoint	Pricing depends on number of servers and platform, but typically is around \$5,000	MOSS 2007 and SharePoint 2010; limited support for SPS 2003. (Also offers Sharelink for SharePoint to migrate Livelihood ECM data.)	Server-side install	Yes, private cloud/ hosted	Partial	Partial	Yes	Yes	

Map Metadata During Migration? Map Users During Migration? Map Site and List Templates During Migration?	Connect to Multiple Sites?	Pre-Migration Tools?	Ability to Migrate Remotely?	Ability to Batch Operations/Schedule Jobs?	Live Migration Option?	Incremental Migrations?	Migrate from Backups?	Windows PowerShell Enabled?	Delegate/Distribute Workload?	Compare Data?	Roll-Back Option?	Site Creation?
Map metadata during migration? Yes; configuration files can be uploaded to the UI to streamline process. Map users during migration? Yes; configuration files can be uploaded to the UI; mapping 'profiles' must be configured before migration is executed Map site and list templates during migration? Yes; customizable; must be configured before migration runs	Can select multiple nodes, etc., for migration; on the destination side, can select one node, so select higher levels and auto-create sites underneath to mirror the destination, or can granularly select source sites, and map into one destination. Currently pulls content from one source at a time, so selecting multiple sites across MOSS 2007 farms, for instance, isn't currently supported.	Yes	Yes, browser-based access with unique login credentials and user permissions; optional integration with Active Directory	Yes	Yes	Yes	Yes	Powershell/CLI-enabled migration includes Lotus Notes, SPS 2003 to SharePoint 2010; planned soon for MOSS 2007 to SharePoint 2010	Yes	Yes	Yes	Yes
Map metadata during migration? No, however it migrates all historic metadata, and support for mapping metadata is targeted for the next release Map users during migration? Yes Map site and list templates during migration? No, however it is targeted for the next release	Yes	Yes	Yes, web interface	Yes, offers scheduling engine; can create SharePoint migration sets and manage in batches; can migrate in waves, based on user-defined timetables, priorities, and severity of issues	Yes, supports migrations on live systems; no need to lockdown the environment to plan, organize, or execute a migration.	Yes	No	No	Yes	Yes	No, however it doesn't delete or remove source data, so admins can test migrations as needed, and delete the 2010 test site and data	No, but support for site creation is targeted for next release
Map metadata during migration? Yes Map users during migration? Yes Map site and list templates during migration? Yes	Yes	No	Yes	Yes, via PowerShell scripts	Yes	Yes	No	Yes	Yes, users can migrate only what they have access to	Yes, by using SharePoint information architect product available as part of complete SharePoint migration suite	No	Yes
Map metadata during migration? Yes Map users during migration? Yes Map site and list templates during migration? Yes	Yes	Yes, in Website Migration Manager and FileShare Migration Manager	Yes, browser-accessible SharePoint sites including those outside organization's intranet	Yes, can batch multiple list migration operations and re-run at any time; after a job is created, can write a PowerShell script and customize or execute it along with other processes	Yes, can point to an unattached database, extract the data directly, and migrate it into a live SharePoint 2010 environment	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Map metadata during migration? Yes Map users during migration? Yes Map site and list templates during migration? Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes, by using MetaVis Live Compare dialog available in MetaVis Change Control and Release Manager	Yes	Yes
Map metadata during migration? No Map users during migration? Yes, for version upgrades (2003-2007/2010 and 2007-2010) Map site and list templates during migration? Yes (via an XML file)	Yes	Yes	Yes, can connect to the Migration Manager web console and remotely configure, track, and manage migration jobs using a web browser	Yes	Yes, all migrations performed live	Yes, automatic post-migration synchronization	No	No	Yes, access to the product web console can be delegated	Yes	No	Yes
Map metadata during migration? Yes Map users during migration? Yes Map site and list templates during migration? Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes

THE CONVERSATION BEGINS HERE



BONUS: Cloud
& Mobile App sessions



**Karlsruhe
Germany**

9-10 June 2011

8 June
Workshops

London, UK

14-15 June, 2011

13 June
Workshops

DEVELOPERS • IT PROS • IT MANAGERS

- Train with 50+ Microsoft and industry experts at over 115 deep dive sessions
- Attend cutting edge keynotes and keep your competitive edge
- Network with speakers, partners and colleagues
- Attend the co-located event sessions at **no extra charge**

KEYNOTE SPEAKERS



STEVE FOX
Microsoft
Director, Developer and
Platform Evangelism
for SharePoint

DAVE MENDLEN
Microsoft
Senior Director
Developer Platform
and Tools

SCOTT GUTHRIE
Microsoft
Corporate
Vice President
.NET Developer
Platform

TONY REDMOND
Tony Redmond
and Associates

Providing the vision and intelligence to keep you and your company competitive in today's market!

A SAMPLING OF OUR INDUSTRY EXPERTS



DAN HOLME
Intelliem, Inc.



**WOUTER
VAN VUGT**
code-counsel



JUVAL LOWY
IDesign, Inc.



DINO ESPOSITO
IDesign Inc.



SCOT HILLIER
Scot Hillier Technical
Solutions, LLC.



STEFFEN KRAUSE
Microsoft
Deutschland GmbH



**DANIEL
MELANCHTHON**
Microsoft
Deutschland GmbH



AGNES MOLNAR
BA Insight



REINER GANSER
Ganser
IT-Consulting



BILLY HOLLIS
Author



NENO LOJE
www.teamssystem
pro.com



**PETER
MONADJEMI**
activetraining



JOHN PAPA
Microsoft



PAUL S. RANDAL
SQLskills.com



**KIMBERLY L.
TRIPP**
SQLskills.com



CHRISTIAN WENZ
Arrabiata
Solutions GmbH

Check the Web site for the full list of sessions and speakers

QUESTIONS ANSWERED • STRATEGY DEFINED • RELATIONSHIPS BUILT

SPACE IS LIMITED Register Today! Call +44 (0)161 929 2800 |
www.DevConnections.com/Germany | www.DevConnections.com/UK

POWERED BY MICROSOFT, DEVCONNECTIONS AND ITCONNECTIONS

■ Exchange

■ Green Computing

■ Security

INSIGHTS FROM THE INDUSTRY

Lessons Learned about Exchange 2010 Migrations, DAG Lag Copies, Lync, and More

This past March, I spent several days at the Microsoft Exchange Connections conference in Orlando. I was able to attend several of the sessions, which were packed with great content about Exchange Server, Lync, and telephony for Exchange admins.

The first full day of sessions at Connections is "Microsoft Day," which means that sessions in all the tracks are presented by speakers from Microsoft or picked by Microsoft. Perhaps the biggest news that came out of these sessions is that Microsoft IT is no longer using lag copies with its database availability groups (DAGs). Dupuy said that Microsoft no longer necessarily recommends lag copies as a backup strategy for Exchange data, and if you choose to implement them, you should have a solid justification based on your organizational size, available hardware, and so forth. Tony Redmond reiterated this point during his keynote for the Exchange track the next morning, saying essentially that lag copies are "an interesting exercise in computer science" but there are better point-in-time backup and restore solutions available on the market.

After lunch, I switched over to Harold Wong's session on Lync 2010. It's great to see a speaker who is so passionate about the technology and able to explain it in a meaningful way. In the session I attended, Wong demoed how quickly and easily you could switch devices during a Lync call, without needing to reconnect. I was also impressed with the Lync feature that lets you record not just voice but entire shared presentations—video, PowerPoint, etc.—and store that recording to your local drive. I could definitely use a feature like that!

Migration to Exchange Server 2010 is clearly one of the major topics around Exchange at the moment, and several

sessions touched on this point—beginning with Redmond's keynote, "Six Critical Issues for Successful Exchange 2010 Deployments." A few of the takeaways from the keynote include:

- It's critical to get to know the Mailbox Replication Service (MRS) for successful Exchange 2010 migration.
- When planning your migration don't forget about third-party products, connectors, log analyzers, add-ons, and anything else that touches Exchange.
- You've got to consider what client you'll provide for your end users—don't bother with Outlook 2003; stick with Outlook 2010 or Outlook 2007. OWA 2010 is a worthwhile option to avoid using a desktop client.
- If you're already on SAN storage, stay on SAN for great performance; if you need to buy new storage, consider DAS for Exchange. JBOD, although technically possible, will require a lot of hands on administration.

To round out his talk, Redmond discussed the possibility of moving your Exchange organization to the cloud. It's been my experience that most Exchange admins aren't in favor of such a move; however, when it comes time to make a decision about the cloud, in many cases it's a company's messaging system that makes the most sense to move. So, Redmond's recommendation is to learn and do many things within your IT organization.

Jim McBee presented a session about "Migrating to Exchange 2010 from Exchange 2003." The focus of this session was on what you can do in your environment now to prepare for a planned move—and save yourself headaches later on. One of McBee's big points was

to ensure that your Active Directory (AD) sites and subnets are defined correctly. As McBee said, "Exchange 2010 will expose any potential problems in Active Directory." He also discussed carefully documenting your current Exchange environment—mail flow, all the software and services that touch Exchange, what clients you have in use, any custom applications you're running—so that you can make decisions about how you'll handle each of these elements on Exchange 2010. McBee also pointed out that you should ensure that your testing or lab environment resembles your actual live environment as closely as possible to avoid unexpected problems.

As I mentioned up front, I'm sure I missed as many great sessions as I was able to attend. For instance, I spotted this note on Twitter: "@billrod: Best session yesterday was Peter O'Dowd amazing talk on exchange store. Looking forward to more great sessions @devconnections."

I did, however, see Peter O'Dowd's session, "Telephony Demystified for Exchange Admins (part 1)," which was a great introduction to this topic. O'Dowd geared his talk toward helping admins overcome the fears associated with implementing some of these features, which can be a little more difficult than your basic email, and he presented the "part 2" session afterward that got more into the how-tos of implementing these features in Exchange 2010.

There was a plethora of great topics and great people to talk to at the conference. And, being a smaller show than something like Microsoft's TechEd gives you a real opportunity to mingle with your peers and the experts/speakers, who have all come to do the same. So, hope to see you at a future show!

—B. K. Winstead

WEB HOSTING. TWICE AS SECURE.

1&1 DUAL H

Double Security, Double Reputability:

No one can afford downtime of their website...

1&1 is now offering dual hosting for the ultimate security of your website. Your website is hosted in two different locations in our data center. If the first location is unexpectedly interrupted, your site will automatically continue running in the second location – without any data loss.



HOSTING

No other web host offers as much expertise, know-how and quality as 1&1: 1&1 combines over 20 years of web hosting experience with the latest technology in our high-speed and high-performance American data center. More than 1,000 IT professionals will continue to develop our top performance web solutions for years to come.

NEW: 1&1 is pleased to offer double security for your website with 1&1 Dual Hosting! All at unbeatably low prices!



**Double Security:
1&1 Dual Hosting**



**Fast Global Network Connectivity:
210 GBit/s Connection**



**Top Performance:
High-end Servers**



**Environmentally Responsible:
100% Renewable Energy**



**Solid Technical Foundation:
Over 1,000 In-house Developers**

NEW!

1&1 DUAL UNLIMITED

- 3 FREE Domains
- FREE Private Domain Registration
- **UNLIMITED** Web Space
- **UNLIMITED** Traffic
- **UNLIMITED** FTP Accounts
- **UNLIMITED** E-mail Accounts (2 GB)
- **UNLIMITED** Mailing Lists
- 20 Microsoft® SQL Databases
- ASP, .NET, AJAX, LINQ, PHP, Perl, SSI
- GeoTrust® Dedicated SSL Certificate
- **NEW!** 1&1 SiteAnalytics
- 99.99% Uptime
- 24/7 Toll-free Customer Support

**1&1 DUAL
UNLIMITED
\$9.99**
per month*
(36 month term)

\$11.99/month (24 month term)
\$12.99/month (12 month term)
\$13.99/month (3 month term)

Please see following page for more
1&1 DUAL HOSTING packages.



1-877-GO-1AND1

www.1and1.com



1-855-CA-1AND1

www.1and1.ca

Touring HP's New Sustainable-Energy Data-Center Research Facility

Two miles down the street from the *Windows IT Pro* offices in Fort Collins, Colorado, HP has opened a new, state-of-the-art research facility in which the company will advance sustainable data center technologies. I got the opportunity to tour the new facility with a few of my colleagues.

HP's goal with the new facility, essentially, is to "go green"—specifically, to expand its Converged Infrastructure architecture by developing technologies that eliminate IT sprawl, increase energy efficiency, and reduce power consumption. All of this is in the interest of helping clients minimize their carbon footprint and reinvest cost savings into their core business. The ultimate goal is to go off-grid by taking strategic advantage of thermal logic and local sources of energy—for example, wind in high-wind environments and the sun in high-solar locations.

The 50,000-square-foot research facility—which is about 75 percent complete—will let HP explore new strategies for reducing the environmental impact of next-generation data centers.

When it's completed, the site will use technologies to help customers minimize power for the cooling of their data centers, while increasing their capacity with less equipment. Chandrakant Patel, HP senior fellow and director of the Sustainable Ecosystems initiative, stresses a holistic approach to the energy challenge—a "cradle-to-cradle," entire-lifecycle perspective toward creating data centers that reduce their consumption of available energy.

The 10-megawatt research center (which holds 10,000 servers) will focus advanced data analytics enabled through fine-grained sensor technology that supports the company's Data Center Smart Grid initiative. HP will also study sophisticated resource management through

the use of power and cooling microgrids. These consist of air- and water-side economizers that take advantage of the Rocky Mountains region's climate. And, according to HP Researcher Cullen Bash, "it's not Colorado's low temperatures that provide the greatest benefits, but actually Colorado's low humidity."

Advancements to reduce power consumption include thousands of environmental sensors for gathering data across the facility, and a water-side economizer providing evaporative cooling through cooling towers (see Figure 1), eliminating the use of a power-intensive compressor. It has hot and cold aisles, and every aisle between rows of server racks is bounded with cool-air intakes or hot-air outlets. Air is brought into the cool aisles from underneath and exhausted



Figure 1: Cooling towers offer more efficient cooling

from the hot aisles overhead to allow for constant air circulation through the racks. Of particular interest were the hundreds of adaptive vent tiles (AVTs) lining the floor, dynamically cooling the racks according to environmental sensors, as Figure 2 shows.

During the tour, we walked into a massive room housing far more power-intensive, backup chiller units, only to find them completely powered down—an energy footprint of zero.

The facility will integrate HP Labs technologies that let customers:

- Reduce energy costs by dynamically adjusting IT, power, and cooling resources as well as integrating supply- and demand-side management systems with existing building management systems.
- Improve management of IT loads and shift resources to where they are needed with a Sustainable Data Center System that includes other advanced technologies such as adaptive vent tiles, fine-grain sensing, and sophisticated management software.

In addition, the facility will house the HP Labs "Sandbox," a research environment that is isolated both environmentally and electronically from the rest of the facility. The Sandbox serves as a test bed for new sustainability technology from HP Labs.

—Jason Bovberg



Figure 2: Adaptive vent tiles increase and decrease air flow as needed

Windows 8 Security Features

There's been a flurry of news in recent days revealing some of the expected new features in Windows 8, with our own Paul Thurrott (and Rafael Rivera from Within Windows) ferreting out some news and sources on their own, while Tom Warren at WinRumors also has some information about potential changes and improvements to Windows 8 on the backup front. There haven't been too many other details come to light about what new security features Windows 8 may include, but there has been enough news and rumors in certain areas to lead us to speculate a bit.

One of the most noteworthy potential new features of Windows 8 from a security perspective could be the new Windows 8 integrated document reader, which will reportedly support PDF (and potentially more) file formats. PDF files and flash plug-ins have been notoriously porous from a security perspective, and Modern Reader may signal a move by Microsoft to add yet even more default security to the Windows platform, a move that would echo recent statements about a move toward enhanced platform security made by other Microsoft executives.

An integrated Microsoft reader would undoubtedly be part of the unified Windows Update OS patching process, which removes the need for users (and admins) to worry about patching products from another vendor using a separate (and non-synchronized) update process, as is the case with Adobe's stand-alone product patching system. That move does fit with Microsoft's recent move to a more aggressive security posture when it comes to making Windows (and other core Microsoft applications) as secure as possible, possibly at the cost of angering Microsoft partners such as Adobe.

Regular system backups are a must for any IT professional, and Microsoft (according to WinRumors) is reportedly making an attempt to make that easier, especially on the client side. Here's what Tom Warren of WinRumors writes about History Vault:

"The feature will allow Windows 8 users to backup files and data automatically using the Shadow Copies function of Windows. According to one person familiar with the company's plans, the backup feature will include the ability to restore to a specific time or date on the system. Users will also be able to select files and restore them to different timestamps."

Windows 7 included a host of important security improvements over Vista and XP, including the Windows 7 action center, a revamped Windows firewall, an improved Windows backup system, improved BitLocker drive encryption and a host of other security improvements. Windows 7 made huge strides on the security front, but will Windows 8 do the same?

If there's a security feature that you hope Windows 8 will have, send me your wish list via email to jeff.james@penton.com or via Twitter @jeffjames3.

—Jeff James

1&1 DUAL HOSTING

SECURE & SAVE!

1&1 DUAL BASIC

- 1 FREE Domain
- 10 GB Web Space
- **UNLIMITED** Traffic
- **NEW!** 5 FTP Accounts
- **NEW!** 1&1 SiteAnalytics

\$2.99
per month*
(36 month term)

\$3.99/month (24 month term)
\$4.99/month (12 month term)
\$6.99/month (3 month term)

1&1 DUAL ADVANCED

- 2 FREE Domains
- 150 GB Web Space
- **UNLIMITED** Traffic
- **NEW!** 50 FTP Accounts
- **NEW!** 1&1 SiteAnalytics

\$4.99
per month*
(36 month term)

\$5.99/month (24 month term)
\$6.99/month (12 month term)
\$8.99/month (3 month term)

.com

Now only \$7.99/first year*

.biz

Now only \$3.99/first year*

1&1 DOMAINS
Starting at

\$3.99
first year*

FREE Private Registration!

*Visit www.1and1.com for full promotional offer details. Program and pricing specifications and availability subject to change without notice.

**More special offers
available online.**



www.1and1.com



www.1and1.ca

1&1®



Thank You to Our SPONSORS

Windows Azure™ Platform



THANK YOU

for sponsoring **mobile, cloud, & virtualization** connections

APRIL 17-20, 2011 | BELLAGIO, LAS VEGAS

AD INDEX

For detailed information about products in this issue of *Windows IT Pro*, visit the web sites listed below.

COMPANY/URL	PAGE	COMPANY/URL	PAGE	COMPANY/URL	PAGE
1&1 Internet	66,67,69	IBM Corporation	Cover 4,9	Penton Media	10
www.1and1.com		www.ibm.com/facts		www.winsupersite.com/go/app	
Altova	Cover 3	Microsoft Corporation	Cover 2	SharePoint Coast-to-Coast Tour	33
www.altova.com		www.microsoft.com/cloud/privatecloud		www.DevConnections.com/SPTour	
Cloud IT ProOnline	36	Mobile Cloud Virtualization Connections ..	70	TCI Europe Events	64
www.CloudITProOnline.com		www.DevConnections.com		www.DevConnections.com/Germany	
Exchange 2010 Essentials Workshop	6	MobileDevProOnline	36	www.DevConnections.com/UK	
www.windowsitpro.com/go/exchange		www.MobileDevProOnline.com		Tower 48, Inc.	3
HP	28	NetWrix Corp	12	www.Tower48.com	
www.hp.com/go/takecontrol4		www.netwrix.com		Windows IT Pro Magazine	10,32,51
				www.windowsitpro.com	

VENDOR DIRECTORY

The following vendors or their products are mentioned in this issue of *Windows IT Pro* on the pages listed below.

App-DNA	53	Intellinet Network Solutions	53	NopSec	53
Apple	53	IObit	52	Quest Software	56
Centrify	52, 56	Iolo Technologies	54	ScriptLogic	52
Cofio Software	52	Lenovo	52	Thursby Software	60
HP	68	Likewise Software	56	VMware	43

DIRECTORY OF SERVICES | WINDOWS IT PRO NETWORK

Search our network of sites dedicated to hands-on technical information for IT professionals.
www.windowsitpro.com

Support

Join our discussion forums. Post your questions and get advice from authors, vendors, and other IT professionals.

www.windowsitpro.com/go/forums

News

Check out the current news and information about Microsoft Windows technologies.

www.windowsitpro.com/go/news

EMAIL NEWSLETTERS

Get free news, commentary, and tips delivered automatically to your desktop.

[asp.netNOW](#)

[DevProConnections UPDATE](#)

[Exchange & Outlook UPDATE](#)

[Security UPDATE](#)

[SharePoint Pro UPDATE](#)

[SQL Server Magazine UPDATE](#)

[Windows IT Pro UPDATE](#)

[Windows Tips & Tricks UPDATE](#)

[WinInfo Daily UPDATE](#)

www.windowsitpro.com/email

RELATED PRODUCTS

Custom Reprint Services

Order reprints of *Windows IT Pro* articles. Diane Madzelonka at Diane.madzelonka@penton.com.

Windows IT Pro VIP

Get exclusive access to over 40,000 articles and solutions on CD and via the Web. Includes FREE access to eBooks and archived eLearning events, plus a subscription to either Windows IT Pro or SQL Server Magazine.

www.windowsitpro.com/go/vipsub

SQL SERVER MAGAZINE

Explore the hottest new features of SQL Server, and discover practical tips and tools.

www.sqlmag.com

ASSOCIATED WEBSITES

DevProConnections

Discover up-to-the-minute expert insights, information on development for IT optimization, and solutions-focused articles at DevProConnections.com, where IT pros creatively and proactively drive business value through technology.

www.devproconnections.com

SharePoint Pro

Dive into Microsoft SharePoint content offered in specialized articles, member forums, expert tips, and Web seminars mentored by a community of peers and professionals.

www.sharepointpromag.com

NEW WAYS TO REACH

WINDOWS IT PRO EDITORS:

LinkedIn: To check out the *Windows IT Pro* group on LinkedIn, sign in on the LinkedIn homepage (www.linkedin.com), select the Search Groups option from the pull-down menu, and use "Windows IT Pro" as your search term.

Facebook: We've created a page on Facebook for *Windows IT Pro*, which you can access at: <http://tinyurl.com/d5bqbf>. Visit our Facebook page to read the latest reader comments, see links to our latest web content, browse our classic cover gallery, and participate in our Facebook discussion board.

Twitter: Visit the *Windows IT Pro* Twitter page at www.twitter.com/windowsitpro.

Windows IT Pro



Ctrl+Alt+Del

by Jason Bovberg

"Send your funny screenshots, industry humor, and hilarious end-user stories to rumors@windowsitpro.com. If we use your submission, you'll receive a free Ctrl+Alt+Del gift."

Coughing Up Hairballs

PRODUCT OF THE MONTH

Does your company run a complex cluster of disparate, conventional, on-premise software? Multiple incompatible software applications? If so, you're probably experiencing "hairballs" of clogged performance. At least, that's the decidedly unconventional choice of words from NetSuite, which claims to offer a proven cure for Software Hairball Syndrome (SHS) by providing a complete cloud-based business system with which to manage your accounting, sales, order management, service, and ecommerce processes. At NetSuite's Hairball Institute for Business, you can download—yes—a Hairball Elimination Kit. Find out more at www.netsuite.com.



Figure 1: Crap—oh wait!

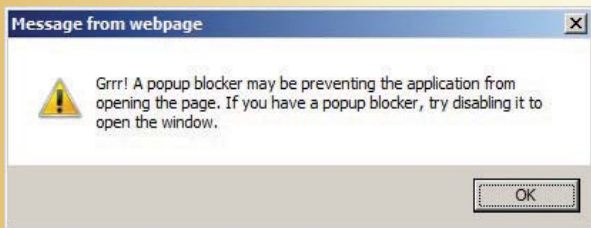


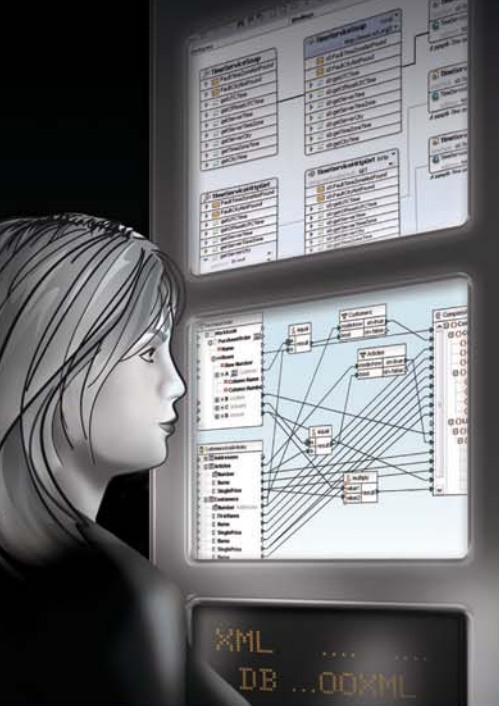
Figure 2: Frustration

USER MOMENT OF THE MONTH

I used to be the sole administrator for a small marketing outfit in Florida. We made those restaurant and event brochures that you find in hotel rooms. One day, our top salesman—to be honest, an older man who had trouble with the more technological aspects of his job—called me to complain that the laptop I'd issued him was too heavy. He was about to take it on a business trip and didn't look forward to lugging all that weight around. He was a gruff old coot, so I half-jokingly tried my luck with, "There's a lot of files on there ... a lot of software. No wonder it's so heavy!" He ended up laboriously removing most of his non-essential files and old email before leaving for his trip. He never brought up the subject again, and I still wonder if he ever realized he'd been played, or if he thought the laptop was appreciably lighter after all his deletions.

—Patrick

June 2011 issue no. 202, *Windows IT Pro* (ISSN 1552-3136) is published monthly. Copyright 2011, Penton Media, Inc., all rights reserved. Windows is a trademark or registered trademark of Microsoft Corporation in the United States and/or other countries, and *Windows IT Pro* is used under license from owner. *Windows IT Pro* is an independent publication not affiliated with Microsoft Corporation. Microsoft Corporation is not responsible in any way for the editorial policy or other contents of the publication. *Windows IT Pro*, 748 Whalers Way, Fort Collins, CO 80525, (800) 793-5697 or (970) 663-4700. Sales and Marketing Offices: 748 Whalers Way, Fort Collins, CO 80525. Advertising rates furnished upon request. Periodicals Class postage paid at Loveland, Colorado, and additional mailing offices. POSTMASTER: Send address changes to *Windows IT Pro*, 748 Whalers Way, Fort Collins, CO 80525. SUBSCRIBERS: Send all inquiries, payments, and address changes to *Windows IT Pro*, Circulation Department, 748 Whalers Way, Fort Collins, CO 80525. Printed in the USA.



Connect legacy technologies affordably with the complete set of data integration tools from Altova®



Experience how the Altova MissionKit®, the integrated suite of XML, data mapping, and database tools, can help you leverage existing technology and business software investments while integrating modern technologies – without breaking your budget.

The Altova MissionKit includes multiple intelligent tools for data integration:

MapForce® – Graphical data mapping, transformation, & conversion tool

- Drag-and-drop data conversion with instant transformation & code gen
- Support for mapping XML, DBs, EDI, Excel®2007+, XBRL, flat files & Web services

XMLSpy® – XML editor and Web services tool

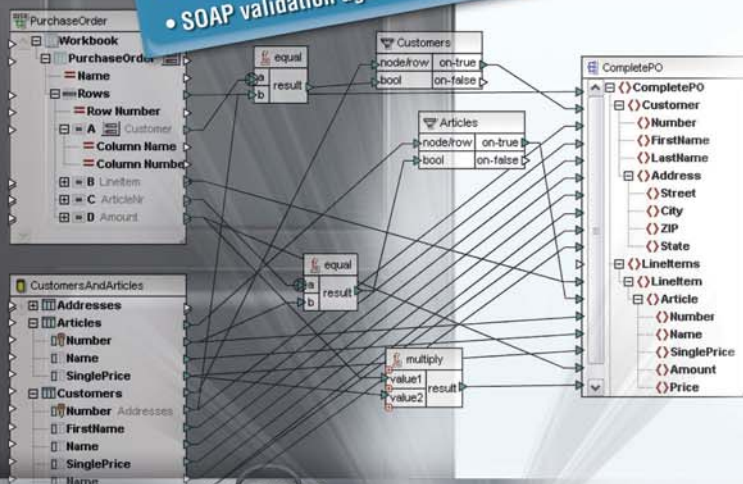
- XML editor with strong database integration
- Web services tool, JSON <> XML converter

DatabaseSpy® – multi-database query, design, comparison tool

- Support for all major relational databases and translation between DB types
- SQL editor, graphical database design & content editor

New in Version 2011:

- Instant chart creation to analyze XML and database data
- StyleVision® integration in MapForce for rendering data mapping results in attractive reports
- Chained data transformations
- Data streaming for ETL
- Support for IATA PADIS EDI
- SOAP validation against WSDL



Download a 30 day free trial!

Try before you buy with a free, fully functional, trial from www.altova.com



Netezza. Up and running in 24 hours, not 24 days.

Get set up in hours instead of days, and start counting returns in minutes instead of hours. All with IBM's Netezza data warehouse appliance for high-performance analytics. It gives you analytics reports at supersonic speeds. At a fraction of the cost of Oracle Exadata. Get real, actionable business results fast.

ibm.com/facts

COST comparison based on publicly available information as of 2/10/2011 for an Oracle Exadata X2-2 HP Full Rack and a full rack of Netezza TwinFin. The cost to acquire Netezza can be as low as 1/6 of Exadata if a client is acquiring new Oracle database licenses and as low as 1/2 if using existing Oracle database licenses. IBM, the IBM logo, ibm.com, Smarter Planet and the planet icon are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml.
© International Business Machines Corporation 2011.